06-30-00 A

Please type a plus sign (+) inside this box +

PTO/SB/05 (4/98)
Approved for use through 09/30/2000. OMB 0651-0032
Patent and Trademark Office: U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number

UTILITY PATENT APPLICATION TRANSMITTAL

(Only for new nonprovisional applications under 37 CFR 1 53(b))

Attorney Docket No.	042390.P7704
First Inventor or Application Identifier	Howard C. Herbert
Title	METHOD FOR SECURE DISTRIBUTION AND CONFIGURATION OF ASYMMETRIC KEYING MATERIAL INTO SEMICONDUCTOR DEVICES
Express Mail Label No.	EL466333398US

APPLICATION ELEMENTS

See MPEP chapter 600 concerning utility patent application contents

ADDRESS TO: Assistant Commissioner for Patents
Box Patent Application
Washington, DC 20231

1. ☒ Fee Transmittal Form
(Submit an original, and a duplicate for fee processing)
2. ☒ Specification [Total Pages 22]
(preferred arrangement set forth below)
   - Descriptive title of the Invention
   - Cross References to Related Applications
   - Statement Regarding Fed sponsored R & D
   - Reference to Microfiche Appendix
   - Background of the Invention
   - Brief Summary of the Invention
   - Brief Description of the Drawings (if filed)
   - Detailed Description
   - Claim(s)
   - Abstract of the Disclosure
3. ☒ Drawing(s) (35 U.S.C. 113) [Total Sheets 11]
4. Oath or Declaration [Total Pages 4]
   a. ☒ Newly executed (original copy)
   b. ☐ Copy from a prior application (37 C.F.R. § 1.63(d)) (for continuation/divisional with Box 16 completed)
      i. ☐ DELETION OF INVENTOR(S)
      Signed statement attached deleting inventor(s) named in the prior application, see 37 CFR §§ 1.63(d)(2) and 1.33(b).

*NOTE FOR ITEMS 1 & 13: IN ORDER TO BE ENTITLED TO PAY SMALL ENTITY FEES, A SMALL ENTITY STATEMENT IS REQUIRED (37 C.F.R. § 1.27), EXCEPT IF ONE FILED IN A PRIOR APPLICATION IS RELIED UPON (37 C.F.R. § 1.28).

5. ☐ Microfiche Computer Program (Appendix)
6. Nucleotide and/or Amino Acid Sequence Submission (if applicable, all necessary)
   a. ☐ Computer Readable Copy
   b. ☐ Paper Copy (identical to computer copy)
   c. ☐ Statement verifying identity of above copies

ACCOMPANYING APPLICATION PARTS

7. ☒ Assignment Papers (cover sheet & document(s))
8. ☐ 37 C.F.R. § 3.73(b) Statement (when there is an assignee) ☐ Power of Attorney
9. ☐ English Translation Document (if applicable)
10. ☐ Information Disclosure Statement (IDS)/PTO - 1449 ☐ Copies of IDS Citations
11. ☐ Preliminary Amendment
12. ☐ Return Receipt Postcard (MPEP 503) (Should be specifically itemized)
13. ☐ *Small Entity Statement(s) ☐ Statement filed in prior application, Status still proper and desired
14. ☐ Certified Copy of Priority Document(s) (if foreign priority is claimed)
15. ☐ Other: ....

16. **If a CONTINUING APPLICATION**, check appropriate box, and supply the requisite information below and in a preliminary amendment:
☐ Continuation ☐ Divisional ☐ Continuation-in-part (CIP) of prior application No:
Prior application Information: Examiner________ Group/Art Unit: ________

For CONTINUATION or DIVISIONAL APPS only: The entire disclosure of the prior application, from which an oath or declaration is supplied under Box 4b, is considered a part of the disclosure of the accompanying continuation or divisional application and is hereby incorporated by reference. The incorporation can only be relied upon when a portion has been inadvertently omitted from the submitted application parts.

17. CORRESPONDENCE ADDRESS

☐ Customer Number of Bar Code Label (Insert Customer No. or Attach bar code label here) or ☒ Correspondence address below

Name	BLAKELY, SOKOLOFF, TAYLOR & ZAFMAN LLP				
Address	12400 Wilshire Boulevard, Seventh Floor				
City	Los Angeles	State	California	Zip Code	90025
Country	U.S.A.	Telephone	(714) 557-3800	Fax	(714) 557-3347

Name (Print/Type)	William W. Schaal, Reg. No. 39,018		
Signature		Date	06/29/00

Burden Hour Statement: This form is estimated to take 0.2 hours to complete. Time will vary depending upon the needs of the individual case. Any comments on the amount of time you are required to complete this form should be sent to the Chief Information Officer, Patent and Trademark Office, Washington, DC 20231. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Assistant Commissioner for Patents, Box Patent Application, Washington, DC 20231.

BSTZ No. 042390.P7704
Express Mail No. EL466333398US

UNITED STATES PATENT APPLICATION

FOR

METHOD FOR SECURE DISTRIBUTION AND CONFIGURATION OF ASYMMETRIC KEYING MATERIAL INTO SEMICONDUCTOR DEVICES

Inventors:

Howard C. Herbert
Derek L. Davis

Prepared by:

Blakely, Sokoloff, Taylor & Zafman LLP
12400 Wilshire Blvd., Suite 700
Los Angeles, California 90025
(714) 557-3800

METHOD FOR SECURE DISTRIBUTION AND CONFIGURATION OF ASYMMETRIC KEYING MATERIAL INTO SEMICONDUCTOR DEVICES

Field

This invention relates to the field of data security.

Background

In today's society, it is becoming increasingly important to transmit data from one location to another in a manner that is clear and unambiguous to a legitimate recipient, but incomprehensible to any illegitimate interlopers. Accordingly, in certain situations, the data is encrypted and thereafter transmitted to the legitimate recipient. At a later time, the legitimate recipient decrypts the transmitted data for use.

One specific process for encrypting and decrypting data is referred to as "asymmetric key cryptography." For asymmetric key cryptography, each device is associated with unique key pair that includes a public key and a private key. A "public key" is used to identify a legitimate recipient of the transmitted data and to encrypt data intended for that recipient. Normally, a "private key" is used to decrypt the encrypted data. Thus, it is essential that the private key is loaded into the device in a secure manner and is held in confidence within the device.

While asymmetric key cryptography provides a mechanism to protect the integrity of data transmitted between two devices, there is no mechanism to ensure that keying material, such as the private key, is loaded into each device in a secure manner. One problem is that the keying material usually is produced at a facility that is remotely located from the facility where an electronic component is packaged. Thus, the transmission of the keying material may be intercepted and/or modified during transit. This poses a security threat, especially when keying material is produced and scheduled for loading into millions of electronic components.

Likewise, there is no current mechanism in place to establish a "configuration window," namely a limited period of validity when an electronic component can be configured with selected keying materials.

BRIEF DESCRIPTION OF THE DRAWINGS

The features and advantages of the present invention will become apparent from the following detailed description of the present invention in which:

Figure 1 is a perspective view of an illustrative embodiment of a distribution network utilizing the present invention.

Figure 2 is an exemplary embodiment illustrating key generation operations by the source.

Figure 3 is an exemplary embodiment illustrating operations performed by the source of Figure 1 to produce a key bundle.

Figure 4 is an exemplary embodiment illustrating operations performed by the source to securely provide configuration encryption keys "CEKs" to the second destination of Figure 1.

Figure 5 is an exemplary embodiment illustrating operations performed by the source to produce BEK_{P2} bundles for transfer to the second destination.

Figure 6 is an exemplary embodiment illustrating operations performed by the source to securely provide sort encryption keys (SEKs) to the first destination of Figure 1.

Figure 7 is an exemplary embodiment illustrating operations performed by the source to encrypt CWIN bundles before transmission to the first destination of Figure 1.

Figure 8 is an exemplary embodiment illustrating operations performed by the source to encrypt BEK_{P1} before transmission to the second destination of Figure 1.

Figure 9 is an exemplary embodiment illustrating operations to securely load keying material into an electronic component.

Figures 10 and 11 illustrate exemplary operations within a reader situated at the first destination.

Figures 12 and 13 illustrate exemplary operations within a reader situated at the second destination.

Figure 14 illustrates exemplary operations to recover and verify the integrity of a first part of a bundle encryption key (BEK_{P1}).

Figure 15 illustrates an exemplary operation to recover keying material from the key bundle.

DESCRIPTION

In general, the present invention relates to a technique for securely transferring data from one location to another and subsequently storing the data within an electronic component. Herein, certain details are set forth in order to provide a thorough understanding of the present invention. It is apparent to a person of ordinary skill in the art, however, that the present invention may be practiced through many embodiments other that those illustrated. Also, well-known circuits are not set forth in detail in order to avoid unnecessarily obscuring the present invention.

In the following description, certain terminology is used to describe features of the present invention. For example, an "electronic component" includes one or more integrated circuits (ICs) having information storage capabilities. In one embodiment, the electronic component is a single IC protected by a semiconductor package, although it is contemplated that the component may be multiple ICs placed within a package, one or more non-packaged ICs, and the like. The information loaded into the electronic component may include one or more encryption/decryption keys in either symmetric or asymmetric form along with supporting digital certificates.

In addition, a "link" is broadly defined as one or more information-carrying mediums (e.g., electrical wire, optical fiber, cable, bus, or air in combination with wireless signaling technology) to establish a communication pathway. This pathway is deemed "secure" when it is virtually impossible to modify information routed over the pathway without such modification being detected. The term "information" is defined as one or more bits of data, address, and/or control. A "bundle" is a collection of information that may include keying material. The term "combined" is generally defined that an arithmetic operation such as concatenation, modular addition, hashing, or another mathematical operation.

With respect to cryptographic functionality, a "cryptographic operation" is an operation performed for additional security on information. These operations may include encryption, decryption, hash computations, and the like. "Keying material" includes any information needed for a specific cryptographic operation such as one or more of the following: (1) a key being a specific series of bits, (2) a key identifier, and (3) an integrity check value.

A "hash operation" is a one-way conversion of information to a fixed-length representation referred to as a "hash value". Often, the hash value is

substantially less in size than the original information. It is contemplated that, in some cases, a 1:1 conversion of the original information may be performed.

In addition, asymmetric key cryptography normally utilizes a root key. A "root public key" is a public key at the origination of a digital certificate chain and provides a starting point for verification of subsequent digital certificates. In general, a "digital certificate" includes information used to authenticate a sender of information. For example, in accordance with CCITT Recommendation X.509: The Directory - Authentication Framework (1988), a digital certificate may include information (e.g., a key) concerning a person or entity being certified, the hash value of which is encrypted using the private key of a certification authority. Examples of a "certification authority" include an original equipment manufacturer (OEM), a software vendor, a trade association, a governmental entity, a bank or any other trusted business or person. A "digital certificate chain" includes an ordered sequence of two or more digital certificates arranged for authorization purposes as described below, where each successive certificate represents the issuer of the preceding certificate.

I. GENERAL ARCHITECTURE

Referring to Figure 1, a perspective view of an illustrative embodiment of a distribution network 100 utilizing the present invention is shown. Distribution network 100 comprises a source 110, a first destination 120 and a second destination 130. Source 110 is in communication with first destination 120 and second destination 130 via links 140 and 150, respectively. It is contemplated that source 110, first destination 120, and/or second destination 130 may be remotely located from each other.

Herein, for one embodiment, source 110 is a system that produces keying material and transfers this keying material to first and second destinations 120 and 130. The transfer may occur via links 140 and 150 as well as placement on one or more portable tokens 160 and 170 (e.g., any programmable data storage device such as a smart card, a magnetic-strip card, a floppy disk, a CD-ROM, and the like). Preferably, portable token(s) 160 and 170 are sent through an out-of-band information delivery mechanism (e.g., UPS®, FED EX®, mail, etc.).

First destination 120 (e.g., a sort facility) is responsible for initial testing of an IC for the electronic component, loading of the IC with a first collection of keying material in a secure manner, and transferring the IC to second destination 130. Second destination 130 (e.g., a configuration facility) is responsible for

configuring the electronic component by loading a second collection of keying material originating from source 110 into the IC. The loading of the second collection of keying material is based on a number of factors, including the presence of the first collection of material, whether the configuration is performed during an appropriate period of validity, whether the integrity of the downloaded information has been compromised, and the like.

II. SECURE DELIVERY PROCESS

Herein, Figures 2-8 illustrate an exemplary embodiment for delivering the first and second collection of keying material in a secure manner from source 110 to first/second destinations 120 and 130 of Figure 1.

Referring now to Figure 2, an exemplary embodiment illustrating key generation operations by source 110 is shown. Initially, a bundle encryption key (BEK) is produced to encrypt a second collection of keying material produced at the source such as a private key (PRK) and an integrity check value associated with the BEK (referred to as "ICV_{BEK}") as described in Figure 3. In one embodiment, a random number generator (e.g., a hardware-based random number generator or a software-based pseudo-random number generator) produces both a first part of the BEK (BEK_{P1}) and a second part of the BEK (BEK_{P2}) as shown in blocks 200 and 210. Acting as a symmetric key, the BEK is produced by performing a logical operation on both BEK_{P1} and BEK_{P2} (block 220). The logical operation may be an exclusive-OR (XOR) operation for example.

Referring now to Figure 3, an exemplary embodiment illustrating operations performed by the source of Figure 1 to produce a key bundle (described below) is shown. A digital certificate chain 300 is provided along with a private key (PRK) 310 that can be used to create digital signatures for the lowest-level certificate of digital certificate chain 300. PRK 310 and digital certificate chain 300 are targeted for loading into non-volatile memory within an electronic component at the second destination 130 of Figure 1. For this embodiment, digital certificate chain 300 includes a multi-level certificate chain (e.g., L1-L4 certificates) for subsequent use in verifying the integrity of digital signatures created using PRK 310. A root certificate 301 is designated as the highest level (L1) certificate. It is contemplated, however, that any certificate hierarchy may be employed.

As described in Figure 3, a representation of this collection of keying material 320 is encrypted using BEK 330 to produce an encrypted result 335

(labeled as "$ENC_{BEK}(PRK,ICV_{BEK})$" where encryption is represented as "ENC"). As shown, keying material 320 includes PRK 310 and ICV_{BEK} 340. ICV_{BEK} 340 is computed by performing a hash operation on PRK 310 and the contents of digital certificate chain 300. Encrypted result 335 accompanied by digital certificate chain 300 (collectively referred to as the "key bundle" 350) is transferred to second destination 130 via link 150 (see Figure 1).

Referring now to Figure 4, an exemplary embodiment illustrating operations performed by the source to securely provide configuration encryption keys "CEKs" to the second destination of Figure 1 is shown. The CEKs are transferred to the second destination in CEK bundles. Each "CEK bundle" is a collection of a CEK, a key identifier associated with the CEK, and an integrity check value for both the CEK and its associated key identifier. Multiple CEK bundles are transferred because normal control policies at the second destination require at least two CEKs to be provided (e.g., a two person control policy) before decrypting a BEK_{P2} bundle (described below).

As shown, in this embodiment, three different configuration encryption keys (CEK_1, CEK_2 and CEK_3) 400, 410, 420 are produced by a random number generator utilized by the source. Also, key identifiers (KID_{C1}, KID_{C2} and KID_{C3}) 430, 440, 450 that correspond to each of the CEKs 400-420 are produced. Herein, a "key identifier" is information that allows decryption hardware and/or software to identify which CEK is placed on a token or used to encrypt packetized information routed to the second destination in a BEK_{P2} bundle format as described below.

For each corresponding CEK 400, 410 and 420, an integrity check value is produced. Each integrity check value is computed by performing a hash operation on a CEK and its corresponding KID. For example, the integrity check value associated with CEK_1 400 (referred to as "ICV_{C1}") 460 is computed by performing a hash operation on both CEK_1 400 and KID_{C1} 430. Likewise, the integrity check values associated with CEK_2 410 and CEK_3 420, namely ICV_{C2} 470 and ICV_{C3} 480, are computed by performing hash operations on CEK_2 410, KID_{C2} 440 and CEK_3 420, KID_{C3} 450 respectively.

After ICV_{C1}, ICV_{C2} and ICV_{C3} 460, 470 and 480 have been computed, a plurality of CEK bundles 490-492 are produced. As previously mentioned, each "CEK bundle" includes a CEK and its corresponding KID and ICV values. For example, in this embodiment, a first CEK (CEK_1) bundle 490 includes KID_{C1} 430, CEK_1 400 and ICV_{C1} 460 while a second CEK (CEK_2) bundle 491 includes KID_{C2}

440, CEK_2 410 and ICV_{C2} 470. A third CEK (CEK_3) bundle 492 includes KID_{C3} 450, CEK_3 420 and ICV_{C3} 480. Each of these CEK bundles 490-492 is stored within separate portable token(s) 170 and distributed to an appropriate member or members at the second destination. The portable token(s) 170 are sent out-of-band (e.g., via mail, UPS®, FED EX®, etc.) as shown in Figure 1.

Referring now to Figure 5, an exemplary embodiment illustrating operations performed by the source to produce BEK_{P2} bundles for transfer to the second destination 130 is shown. In general, each "BEK_{P2} bundle" includes at least BEK_{P2} encrypted using any combination of CEKs.

As shown, key identifiers are initially produced for identifying certain CEK encryption combinations. For example, as shown, a first group key identifier ($KID_{C2,C3}$) 500 is produced. $KID_{C2,C3}$ 500 represents that information, including BEK_{P2}, is encrypted along this pathway using both CEK_2 410 and CEK_3 420. $KID_{C2,C3}$ 500 may be any chosen representation such as, for example, KID_{C2} 440 and KID_{C3} 450 combined, alphanumeric text, a resultant value computed from a bitwise logical operation on KID_{C2} 440 and KID_{C3} 450, and the like. Similarly, a second group key identifier ($KID_{C3,C1}$) 510 represents that information is being encrypted using both CEK_3 420 and CEK_1 400 while a third group key identifier ($KID_{C1,C2}$) 520 represents encryption using both CEK_1 400 and CEK_2 410.

As shown, hash operations are performed on both BEK_{P2} 530 and each of the group key identifiers ($KID_{C2,C3}$ 500; $KID_{C3,C1}$ 510; $KID_{C1,C2}$ 520) to produce corresponding "group" integrity check values ($ICV_{C2,C3}$ 540; $ICV_{C3,C1}$ 550; $ICV_{C1,C2}$ 560). To produce a first configuration sub-bundle 570, $ICV_{C2,C3}$ 540 and BEK_{P2} 530 are encrypted using CEK_2 410, which is represented as "$E_{CEK2}(BEK_{P2}, ICV_{C2,C3})$". Thereafter, first configuration sub-bundle 570 is encrypted using CEK_3 420 and combined with $KID_{C2,C3}$ 500 to produce a first BEK_{P2} bundle 580. Likewise, in order to produce a second configuration sub-bundle 571, both $ICV_{C3,C1}$ 550 and BEK_{P2} 530 are encrypted using CEK_3 420, which is represented as "$E_{CEK3}(BEK_{P2}, ICV_{C3,C1})$". Thereafter, second configuration sub-bundle 571 is encrypted using CEK_1 400 and combined with $KID_{C3,C1}$ 510 to produce a second BEK_{P2} bundle 581. Likewise, to produce a third configuration sub-bundle 572, both $ICV_{C1,C2}$ 560 and BEK_{P2} 530 are encrypted using CEK_1 400, which is represented as "$E_{CEK1}(BEK_{P2}, ICV_{C1,C2})$". Thereafter, third configuration sub-bundle 572 is encrypted using CEK_2 410 and combined with $KID_{C1,C2}$ 520 to produce a third BEK_{P2} bundle 582. These BEK_{P2} bundles 580-582 are sent to second destination via link 150 as shown in Figure 1.

Referring now to Figure 6, an exemplary embodiment illustrating operations performed by the source to securely provide sort encryption keys (SEKs) to the first destination of Figure 1 is shown. The SEKs are transferred to the first destination in SEK bundles. Each "SEK bundle" is a collection of a unique SEK from the set of SEKs, a key identifier associated with that SEK, and an integrity check value of both the SEK and key identifier. Multiple SEK bundles are transferred because the control policies at the first destination require at least two SEKs to be provided (e.g., a two person control policy) before decrypting configuration window (CWIN) bundles.

More specifically, a CWIN bundle including a "current SEK" (SEK_{SC}) and a "next SEK" (SEK_{SN}) as described in Figure 7. Herein, "SEK_{SC}" represents a current period of validity and "SEK_{SN}" represents a future period of validity. This "period of validity" is defined by the rate at which SEK_{SN} is changed in succession. This period of validity may be periodic in nature (e.g., a set number of days, weeks or months) or random. By the use of both SEK_{SC} and SEK_{SN}, a valid window for configuration of an electronic component is established. Of course, when the configuration window is updated (e.g., the future period of validity has lapsed), SEK_{SN} is converted to SEK_{SC} and a new SEK_{SN} is produced. This continues so that no electronic components associated with validity periods outside this configuration window may be configured at a later time.

As shown in Figure 6, in this embodiment, three different sort encryption keys (SEK_1, SEK_2 and SEK_3) 600, 610, 620 are produced by a random number generator utilized by the first destination. Also, key identifiers (KID_{S1}, KID_{S2} and KID_{S3}) 630, 640, 650 that correspond to each of the SEKs produced. These key identifiers 630, 640, 650 allow decryption hardware and/or software to identify which SEK is placed on a token or which SEKs are used to encrypt packetized information routed to the first destination.

For each corresponding sort encryption key 600, 610 and 620, an integrity check value is produced. Each integrity check value is computed by performing a hash operation on a SEK and its corresponding KID. For example, the integrity check value for a first member (ICV_{S1}) 660 is a hash value produced by performing a hash operation on SEK_1 600 and KID_{S1} 630. Likewise, the integrity check values for a second and third entries (ICV_{S2} and ICV_{S3}) 670 and 680 are hash values produced by performing hash operations on SEK_2 610, KID_{S2} 640 and SEK_3 620, KID_{S3} 650 respectively.

After ICV_{S1}, ICV_{S2} and ICV_{S3} 660, 670 and 680 have been computed, a plurality of SEK bundles 690-692 are produced. Each "SEK bundle" includes a SEK and its corresponding KID and ICV values. For example, in this embodiment, a first SEK (SEK_1) bundle 690 includes KID_{S1} 630, SEK_1 600 and ICV_{S1} 660 while a second SEK (SEK_2) bundle 691 includes KID_{S2} 640, SEK_2 610 and ICV_{S2} 670. A third SEK (SEK_3) bundle 692 includes KID_{S3} 650, SEK_3 620 and ICV_{S3} 680. Each of these SEK bundles 690-692 is placed on a portable token and distributed out-of-band to an appropriate member or members at the first destination. The portable token(s) 160 are sent out-of-band as shown in Figure 1.

Referring now to Figure 7, an exemplary embodiment illustrating operations performed by the source to encrypt CWIN bundles before transmission to the first destination of Figure 1 is shown. Initially, key identifiers (KID_{SC}, KID_{SN}) 700 and 710 are produced to represent a SEK_{SC} 720 and a SEK_{SN} 730. Also, group key identifiers ($KID_{S2,S3}$ 740, $KID_{S3,S1}$ 750, $KID_{S1,S2}$ 760) are produced to represent the SEKs used to encrypt a combination of KID_{SC} 700, SEK_{SC} 720, KID_{SN} 710, and SEK_{SN} 730 (referred to as the "configuration window material" 735) for each CWIN bundle 790-792.

As shown, key identifiers are initially produced for identifying certain SEK encryption combinations. For example, as shown, a first group key identifier ($KID_{S2,S3}$) 740 is produced. $KID_{S2,S3}$ 740 is configured to represent that information, including configuration window material 735, is encrypted using both SEK_2 and SEK_3. $KID_{S2,S3}$ 740 may be any chosen representation such as KID_{S2} 640 and KID_{S3} 650 combined, alphanumeric text, a resultant value computed from a bitwise, logical operation on KID_{S2} 640 and KID_{S3} 650, and the like. Similarly, a second group key identifier ($KID_{S3,S1}$) 750 is designed to represent that information is being encrypted using both SEK_3 620 and SEK_1 600 while a third group key identifier ($KID_{S1,S2}$) 760 represents encryption using both SEK_1 610 and SEK_2 620.

As shown, hash operations are performed on configuration window material 735 and each of the group key identifiers ($KID_{S2,S3}$ 740; $KID_{S3,S1}$ 750; $KID_{S1,S2}$ 760) to produce corresponding group integrity check values ($ICV_{S2,S3}$ 770; $ICV_{S3,S1}$ 771; $ICV_{S1,S2}$ 772). To produce a first sort sub-bundle 780, both $ICV_{S2,S3}$ 770 and configuration window material 735 are encrypted using SEK_2 610. Thereafter, first sort sub-bundle 780 is encrypted using SEK_3 620 and combined with $KID_{S2,S3}$ 740 to produce a first CWIN bundle 790. Likewise, in order to produce a second sort sub-bundle 781, both $ICV_{S3,S1}$ 771 and configuration

window material 735 are encrypted using SEK_3 620. Thereafter, second sort sub-bundle 781 is encrypted using SEK_1 600 and combined with $KID_{S3,S1}$ 750 to produce a second CWIN bundle 791. Likewise, to produce a third sort sub-bundle 782, both $ICV_{S1,S2}$ 772 and configuration window material 735 are encrypted using SEK_1 600. Thereafter, third sort sub-bundle 782 is encrypted using SEK_2 610 and combined with $KID_{S1,S2}$ 760 to produce a third CWIN bundle 792. These CWIN bundles 790-792 are sent to the first destination via link 140.

Referring now to Figure 8, an exemplary embodiment illustrating operations performed by the source to encrypt BEK_{P1} 800 before transmission to the second destination of Figure 1 is shown. To limit the scope of key compromise, short periods of validity should be used for all keys. By encrypting BEK_{P1} 800 with two sort encryption keys whose value changes periodically, namely SEK_{SC} 720 and SEK_{SN} 730, a valid configuration window is created for a given electronic component. In particular, at a predetermined or randomly chosen moment, source 110 replaces the value associated with SEK_{SC} 720 with SEK_{SN} 730 and a new SEK_{SN} 730 is generated.

As shown, BEK_{P1} 800 and KID_{SC} 700 undergo a hash operation, which produces an integrity check value for the SEK_{SC} (referred to as "ICV_{SC}") 810. Both ICV_{SC} 810 and BEK_{P1} 800 are encrypted using SEK_{SC} 720 and combined with KID_{SC} 700 to produce a first BEK_{P1} bundle 820. Concurrently, BEK_{P1} 800 and KID_{SN} 710 undergo a hash operation, which produces an integrity check value for SEK_{SN} (referred to as "ICV_{SN}") 830. Both ICV_{SN} 830 and BEK_{P1} 800 are encrypted using SEK_{SN} 730 and combined with KID_{SN} 710 to produce a second BEK_{P1} bundle 840. First and second BEK_{P1} bundles 820 and 840 are separately loaded within the electronic component as keying material for internal decryption operations (see Figure 9A and 9B).

III. SECURE RECOVERY PROCESS

A. Recovery of SEK_{SC} and SEK_{SN}

This operation takes place at the first destination 120. Referring now to Figures 9A, 10, and 11, for this illustrative example, the first and second operators assigned with SEK_1 and SEK_2 are present to facilitate recovery of SEK_{SC} 720 and SEK_{SN} 730. Upon placement of their tokens 160_1 and 160_2 into a sort system 900, the validity of the data in tokens 160_1 and 160_2 is tested. In particular, as shown in Figure 10, KID_{S1} 630 and SEK_1 600 from SEK_1 bundle 690 (stored in token 160_1)

undergo a hash operation to produce a first test hash value 910. The first test hash value 910 is compared with ICV_{S1} 660 that is part of SEK_1 bundle 690. Additionally, KID_{S2} 640 and SEK_2 610 from SEK_2 bundle 691 (stored in token 160_2) may undergo a hash operation to produce a second test hash value 920. Second test hash value 920 is compared with ICV_{S2} 670 that is part of SEK_2 bundle 691. If matches are detected between both (i) ICV_{S1} 660 and first test hash value 910 and (ii) ICV_{S2} 670 and second test hash value 920, sort system 900 proceeds to attempt recovery of SEK_{SC} and SEK_{SN} from CWIN bundles 790-792. Otherwise, a warning may be issued to indicate that the contents of one or both of the tokens are invalid.

To recover SEK_{SC} and SEK_{SN}, as shown in Figure 11, application software within sort system 900 is provided with SEK_1 and SEK_2 (stored in the tokens) and determines that it can decrypt third CWIN bundle 792 after reading $KID_{S1,S2}$ 760. Third CWIN bundle 792 is decrypted (where decryption is represented as "DEC") to recover KID_{SC} 700, SEK_{SC} 720, KID_{SN} 710, SEK_{SN} 730 and $ICV_{S1,S2}$ 760. The integrity of third CWIN bundle 792 is verified by performing a hash operation on $KID_{S1,S2}$ 760, KID_{SC} 700, SEK_{SC} 720, KID_{SN} 710 and SEK_{SN} 730 to produce a third test hash value 930. Third test hash value 930 is compared to $ICV_{S1,S2}$ 760 and if a match is detected, SEK_{SC} 720 and SEK_{SN} 730 are loaded into non-volatile memory 1005 within electronic component 1000. After the loading of SEK_{SC} 720 and SEK_{SN} 730, electronic component 1000 is transferred to the second destination for loading of the key bundle 350 of Figure 3.

As an alternative, it is contemplated that above-described authentication functions involving contents of the SEK bundles 690-692 and CWIN bundles 790-792 may be performed within the tokens 160 themselves, in lieu of the sort system 900.

B. Recovery of BEK_{P2}

This operation takes place in the second destination 130. Referring now to Figures 9B, 12 and 13, for this illustrative example, the second and third operators assigned with CEK_2 and CEK_3 are present to facilitate the recovery of BEK_{P2}. Upon placement of their tokens 170_2 and 170_3 into a configuration system 905, the validity of the data in tokens 170_2 and 170_3 is tested. In particular, as shown in Figure 12, KID_{C2} 440 and CEK_2 410 from the CEK_2 bundle 491 (stored in token 170_2) undergo a hash operation to produce a fourth test hash value 940. Fourth test hash value 940 is compared with ICV_{C2} 470. Additionally, KID_{C3} 450 and

CEK_3 420 from CEK_3 bundle 492 (stored in token 170_3) undergo a hash operation to produce a fifth test hash value 950. The fifth test hash value is compared with ICV_{C3} 480. If matches are detected between both (i) ICV_{C2} 470 and the fourth test hash value 940 and (ii) ICV_{C3} 480 and the fifth test hash value 950, configuration system 905 proceeds to attempt recovery of BEK_{P2} 530 from BEK_{P2} bundles 580-582. Otherwise, a warning may be issued to indicate that the contents of one or both tokens are invalid.

As shown in Figure 13, to recover BEK_{P2} 530, application software within configuration system 905 is provided with CEK_2 and CEK_3 and identifies that it can decrypt first BEK_{P2} bundle 580 after reading $KID_{C2,C3}$ 500. First BEK_{P2} bundle 580 is decrypted using CEK_3 420 and CEK_2 410 to recover BEK_{P2} 530 and $ICV_{C2,C3}$ 540. The integrity of first BEK_{P2} bundle 580 is verified by performing a hash operation on both BEK_{P2} 530 and $KID_{C2,C3}$ 500 to obtain a sixth test hash value 960. Sixth test hash value 960 is compared to $ICV_{C2,C3}$ 540, which is part of first BEK_{P2} bundle 580. If a match is detected, BEK_{P2} 530 is loaded into volatile memory within electronic component 1000.

As an alternative, it is contemplated that above-described authentication functions involving contents of the CEK bundles 490-492 and BEK_{P2} bundles 580-582 may be performed within the tokens 170 themselves, in lieu of the configuration system 905.

C. Recovery of BEK_{P1}

Referring to Figure 9B and 14, electronic component 1000 is provided with BEK_{P1} bundles 820 and 840. As set forth in Figure 8, a first BEK_{P1} bundle 820 includes KID_{SC} 700 and a result of BEK_{P1} 800 and ICV_{SC} 810 encrypted using SEK_{SC} 720. Second BEK_{P1} bundle 840 includes KID_{SN} 710 and a result of BEK_{P1} 800 and ICV_{SN} 830 encrypted using SEK_{SN} 730. Since SEK_{SC} 720 and SEK_{SN} 730 were loaded into non-volatile memory 1005 within electronic component 1000 during the sort process, first and second BEK_{P1} bundles 820 and 840 can be decrypted to recover BEK_{P1}.

In particular as shown in Figure 14, first BEK_{P1} bundle 820 is decrypted using SEK_{SC} 720 to recover BEK_{P1} 800 and ICV_{SC} 810 from that bundle. The integrity of first BEK_{P1} bundle 820 can be verified by performing a hash operation on both KID_{SC} and BEK_{P1} to produce a seventh test hash value 970 and comparing seventh test hash value 970 with ICV_{SC} 810. If a match is detected, BEK_{P1} 800 is verified and stored in volatile memory within electronic component 1000. If a

match is not detected, the second BEK_{P1} bundle 840 is decrypted using SEK_{SN} 730 to recover BEK_{P1} 800 and ICV_{SN} 830. The integrity of second BEK_{P1} bundle 840 can be verified by performing a hash operation on both BEK_{P1} 800 and KID_{SN} 710. This produces an eighth test hash value 980. Then, eighth test hash value 980 is compared to ICV_{SN} 830. If a match is detected, BEK_{P1} 800 is verified and stored in volatile memory within electronic component 1000.

Although not shown, it is contemplated that BEK_{P1} 800 cannot be recovered if neither the SEK_{SC} nor the SEK_{SN}, when configuring the BEK_{P1} bundles 800, is equivalent to SEK_{SC} 720 and SEK_{SN} 730 loaded within the material (e.g., electronic component 1000) at the first destination. This could prevent invalid configuration of stolen components.

D. Recovery of BEK

Referring still to Figure 9B, an exemplary embodiment of the recovery of BEK is shown. As described above, BEK_{P1} 800 is accessed from internal volatile memory within electronic component 1000 while BEK_{P2} 530 is loaded by electronic component 1000 into its volatile memory from configuration system 905. Within electronic component 1000, a logical operation (e.g., an XOR) 1010 is performed on both BEK_{P1} 800 and BEK_{P2} 530. This produces BEK 330.

E. Recovery of PRK and Digital Certificate Chain

Referring to Figures 3, 9B, 14 and 15, an exemplary embodiment illustrating operations to recover PRK 310 and digital certificate chain 300 is shown. Key bundle 350 is loaded into electronic component 1000. Since BEK 330 has been computed, it is contemplated that PRK 310 and ICV_{BEK} 340 can be recovered from encrypted result 335 that is stored in key bundle 350. This allows the integrity of key bundle 350 to be verified by computing a hash operation of the recovered PRK 310 and digital certificate chain 300 that accompanies encrypted result 335. If the computed hash value 1050 matches ICV_{BEK} 340, the contents of key bundle 350 are valid. Thus, PRK 310 and digital certificate chain 300 are stored in non-volatile memory 1005 within electronic component 1000. Once that is completed, SEK_{SC} and SEK_{SN} are erased from non-volatile memory 1005.

While this invention has been described with reference to illustrative embodiments, this description is not intended to be construed in a limiting sense. Various modifications of the illustrative embodiments, as well as other embodiments of the invention, which are apparent to persons skilled in the art to

which the invention pertains are deemed to lie within the spirit and scope of the invention.

CLAIMS

What is claimed is:

1. A method comprising:

storing a current sort encryption key (SEK) at a first destination in an internal memory of an electronic component;

storing a next SEK at the first destination in the internal memory;

providing the electronic component to a second destination; and

recovering a private key at the second destination from a key bundle based on the current SEK, the next SEK and a plurality of bundles received at the second destination.

2. The method of claim 1, wherein prior to storing the current SEK at the first destination, the method further comprises:

transferring at least a first bundle to the first destination via a first link; and

transferring at least a second bundle to the first destination via a first out-of-band information carrying mechanism.

3. The method of claim 2, wherein the first bundle includes a plurality of configuration window (CWIN) bundles.

4. The method of claim 3, wherein each of the CWIN bundles includes a configuration window material, the configuration window includes (i) a first key identifier associated with the current SEK, (ii) the current SEK, (iii) a second key identifier associated with the next SEK, (iv) the next SEK and (v) a group integrity check value for a first encryption key and a second encryption key.

5. The method of claim 4, wherein the configuration window material is encrypted with the first encryption key and the second encryption key.

6. The method of claim 5, wherein each CWIN bundle further includes a group identifier associated with the first encryption key and the second encryption key.

7. The method of claim 3, wherein the second bundle includes a plurality of sort encryption key (SEK) bundles.

8. The method of claim 7, wherein each of the SEK bundles includes (i) a sort encryption key, (ii) a key identifier associated with the sort encryption key and (iii) an integrity check value associated with the sort encryption key.

9. The method of claim 2, wherein prior to storing the current SEK at the first destination, the method further comprises:

transferring the plurality of bundles to the second destination, the plurality of bundles includes a third bundle and a fourth bundle.

10. The method of claim 9, wherein the third bundle is transferred to the second destination via a second link.

11. The method of claim 9, wherein the fourth bundle is transferred to the second destination via a second out-of-band information carrying medium.

12. The method of claim 9, wherein the third bundle is a plurality of second part bundle encryption key (BEK_{p2}) bundles, each of the BEK_{p2} bundles includes a second part of the bundle encryption key and a combined integrity check value associated with a first encryption key and a second encryption key.

13. The method of claim 12, wherein the second part of the bundle encryption key and the combined integrity check value are encrypted with the first encryption key and the second encryption key.

14. The method of claim 12, wherein each BEK_{P2} bundle further includes a group identifier associated with the first encryption key and the second encryption key.

15 The method of claim 9, wherein the fourth bundle includes a plurality of configuration encryption key (CEK) bundles.

16. The method of claim 15, wherein each of the CEK bundles includes (i) a configuration encryption key, (ii) a key identifier associated with the configuration encryption key and (iii) an integrity check value associated with the configuration encryption key.

17. A method comprising:

at a first destination, recovering a current sort encryption key (SEK) and a next SEK based on information within a first plurality of incoming bundles and storing the current SEK and the next SEK in an internal memory of an electronic component; and

at a second destination, upon receipt of the electronic component, recovering a private key from a key bundle based on the current SEK, the next SEK and a second plurality of incoming bundles.

18. The method of claim 17, wherein the current SEK represents a current period of validity for configuration of the electronic component.

19. The method of claim 17, wherein the next SEK represents a next period of validity for configuration of the electronic component.

20. The method of claim 19, wherein the private key is prevented from being recovered if the next period of validity has lapsed.

21. The method of claim 17, wherein the first plurality of incoming bundles includes a plurality of configuration window (CWIN) bundles.

22. The method of claim 21, wherein each of the CWIN bundles includes (i) a first key identifier associated with the current SEK, (ii) the current SEK, (iii) a second key identifier associated with the next SEK, (iv) the next SEK

and (v) a group integrity check value for a first encryption key and a second encryption key.

23. The method of claim 22, wherein the first key identifier, the current SEK, the second key identifier, the next SEK and the group integrity check value are encrypted with the first encryption key and the second encryption key.

24. The method of claim 23, wherein each CWIN bundle further includes a group identifier associated with the first encryption key and the second encryption key.

25. The method of claim 17, wherein the first plurality of incoming bundles includes a plurality of sort encryption key (SEK) bundles.

26. The method of claim 25, wherein each of the SEK bundles includes (i) a sort encryption key, (ii) a key identifier associated with the sort encryption key, (iii) an integrity check value associated with the sort encryption key.

27. The method of claim 17, wherein the second plurality of bundles includes a plurality of first part bundle encryption key (BEK_{p2}) bundles and a plurality of second part bundle encryption key (BEK_{P2}) bundles.

28. The method of claim 27, wherein each of the BEK_{P2} bundles includes a second part of the bundle encryption key and a group integrity check value for a first encryption key and a second encryption key.

29. The method of claim 28, wherein one of the BEK_{p2} bundles includes a first part of the bundle encryption key and an integrity check value associated with the current SEK.

30. The method of claim 29, wherein one of the BEK_{p2} bundles includes a first part of the bundle encryption key and an integrity check value associated with the next SEK.

31. The method of claim 30, wherein the bundle encryption key is recovered upon recovering the first and second parts of the bundle encryption key.

32. The method of claim 31, wherein the private key is recovered using the bundle encryption key.

33. A method comprising:

receiving at least a first bundle via a first link;

receiving at least a second bundle via a first out-of-band information carrying mechanism;

recovering a current sort encryption key (SEK) and a next SEK based on information contained in the first bundle and the second bundle; and

storing the current SEK and the next SEK in an internal memory of an electronic component.

34. The method of claim 33, further comprising transferring the electronic component to a second destination.

35. The method of claim 34 further comprising receiving at least a third bundle via a second link;

receiving at least a fourth bundle via a second out-of-band information carrying medium;

recovering based on information in the third bundle, fourth bundle, the current SEK and the next SEK.

36. The method of claim 35 further comprising recovering a private key based on the bundle encryption key.

37. A network comprising:

a source to output a first collection of encrypted keying material and a second collection of encrypted keying material;

a first destination to receive the first collection of encrypted keying material, to decrypt keying material originating from the first collection of encrypted keying material for recovery of sort encryption keying material and to store the sort encryption keying material into an internal memory of an electronic component; and

a second destination to receive the second collection of encrypted keying material, to decrypt keying material originating from the second collection of encrypted keying material for recovery of at least private key for subsequent loading in the internal memory.

38. The network of claim 37, wherein the first destination is physically separated from the second destination.

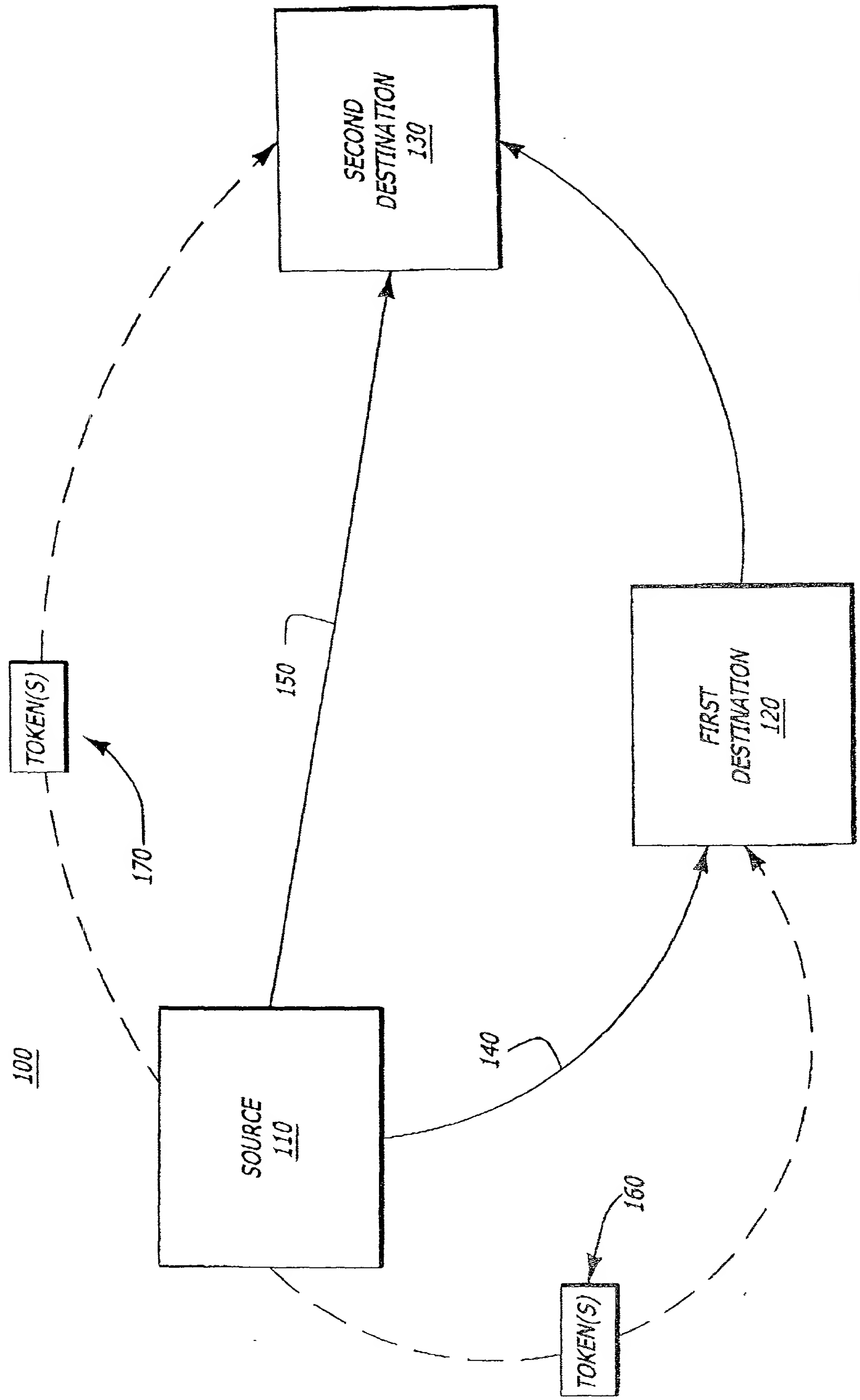
39. The network of claim 37, wherein the sort encryption keying material includes a current sort encryption key (SEK) and a next SEK.

40. The network of claim 39, wherein the current SEK and the next SEK collectively represents a period of validity in which the electronic component must be configured.

41. The network of claim 37, wherein the second destination further recovers a digital certificate chain from the second collection of keying material and loads the digital certificate chain into the internal memory.

ABSTRACT

In one embodiment, a method is described to secure transfer data from one location to another for storage in an electronic component. The transfer occurs with part of the data routed to a first destination and the remaining data routed to a second destination. The data routed to the first destination is for securely loading a current sort encrypted key (SEK) and a next SEK into memory of the electronic component. The data routed to the second destination includes a private key which is recovered using the current SEK and the next SEK.



SECOND DESTINATION 130
FIRST DESTINATION 120
SOURCE 110
TOKEN(S)
TOKEN(S)
100
140
150
160
170

FIG. 1

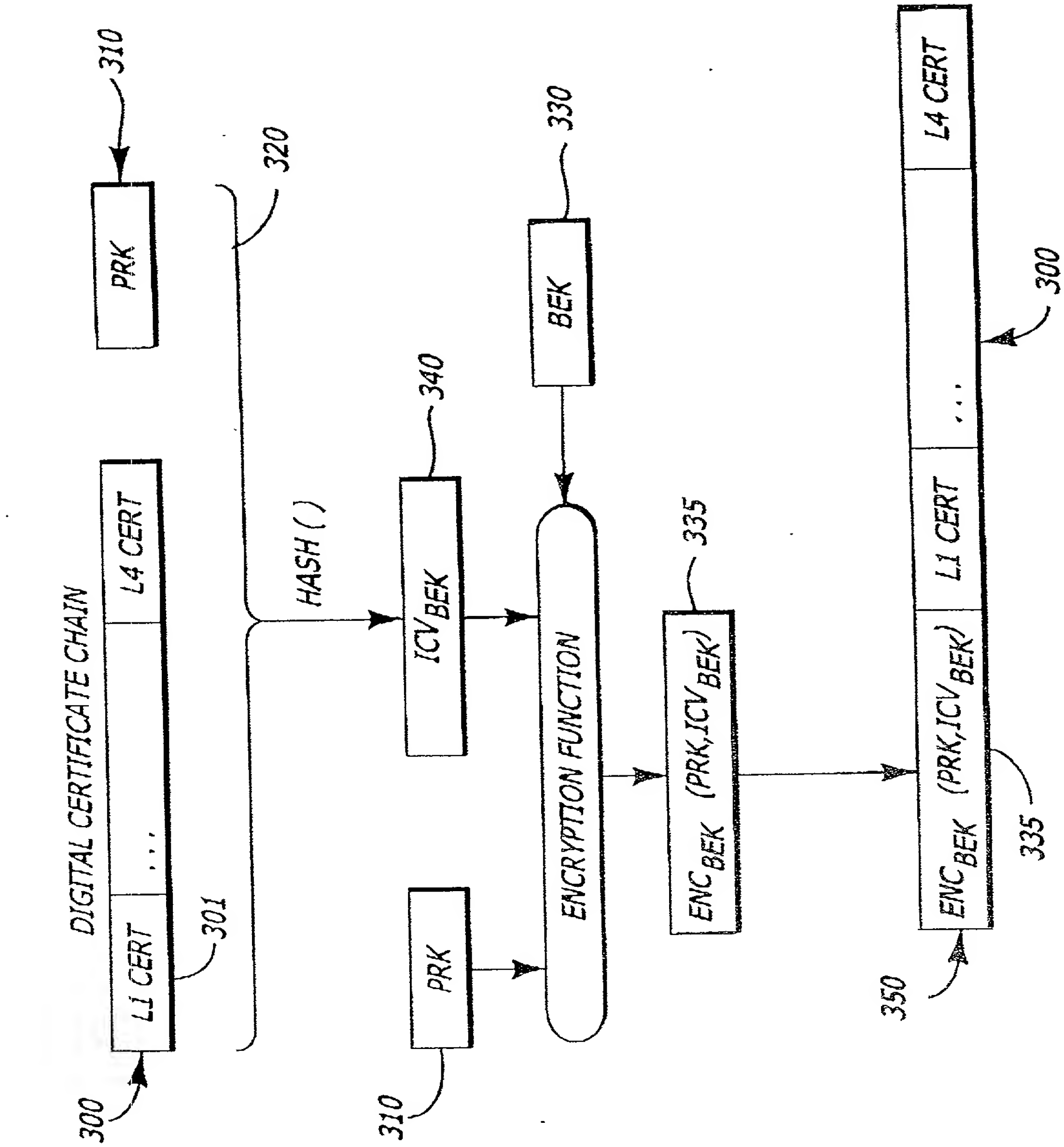

310
PRK
320
DIGITAL CERTIFICATE CHAIN
L1 CERT
...
L4 CERT
301
300
HASH ( )
340
ICV_{BEK}
330
BEK
310
PRK
ENCRYPTION FUNCTION
335
ENC_{BEK} (PRK, ICV_{BEK})
300
L4 CERT
...
L1 CERT
ENC_{BEK} (PRK, ICV_{BEK})
335
350

FIG. 3

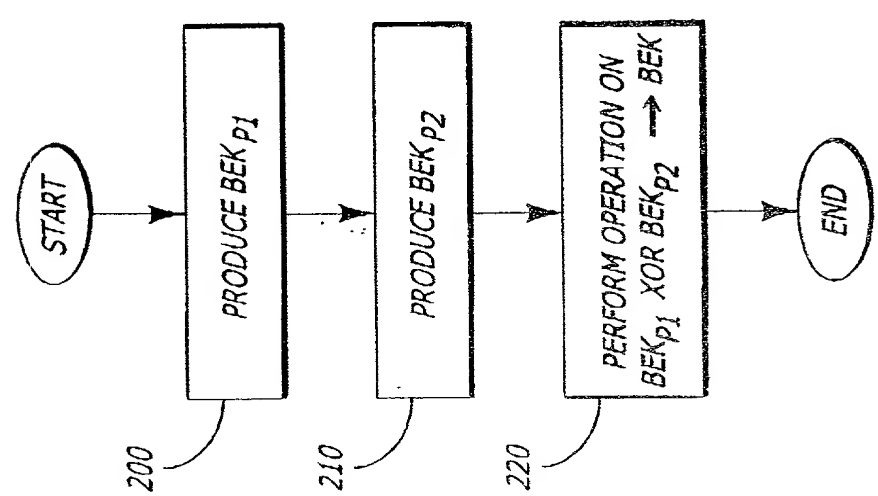
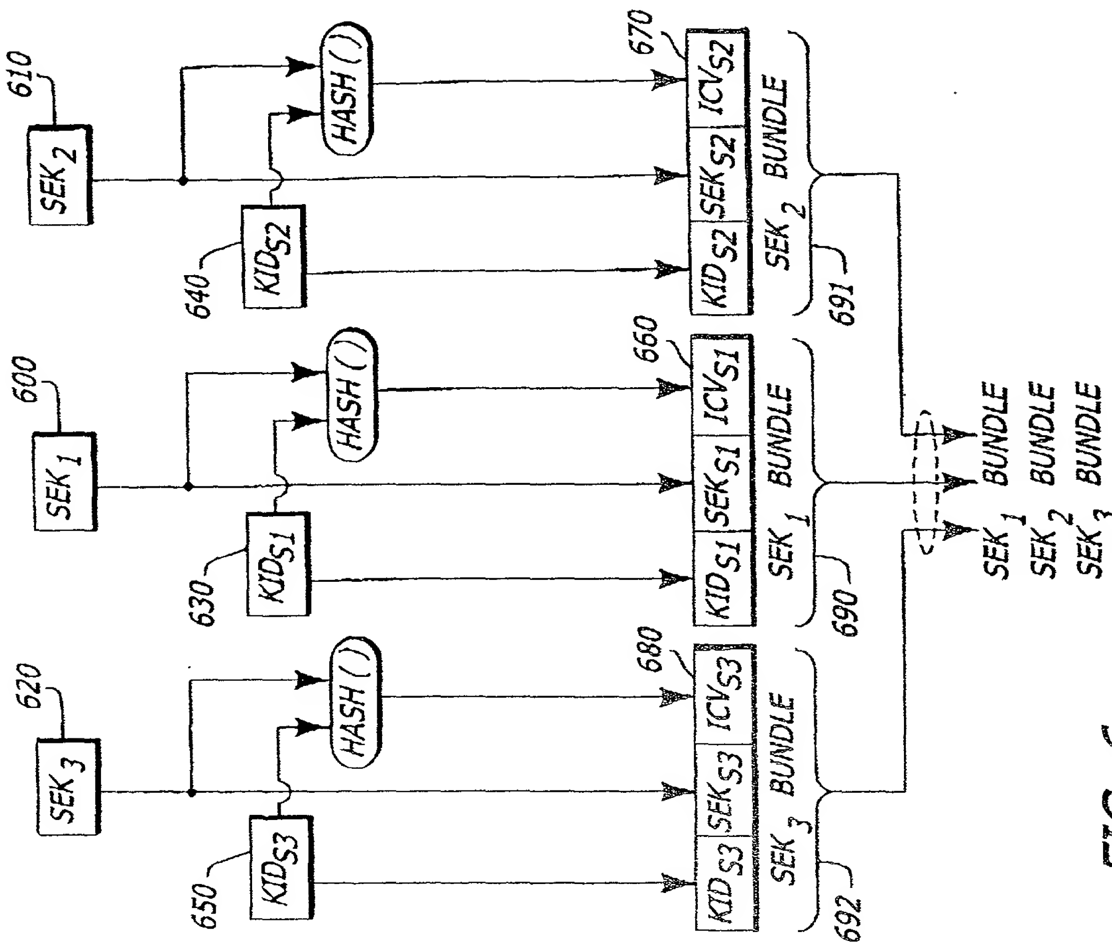
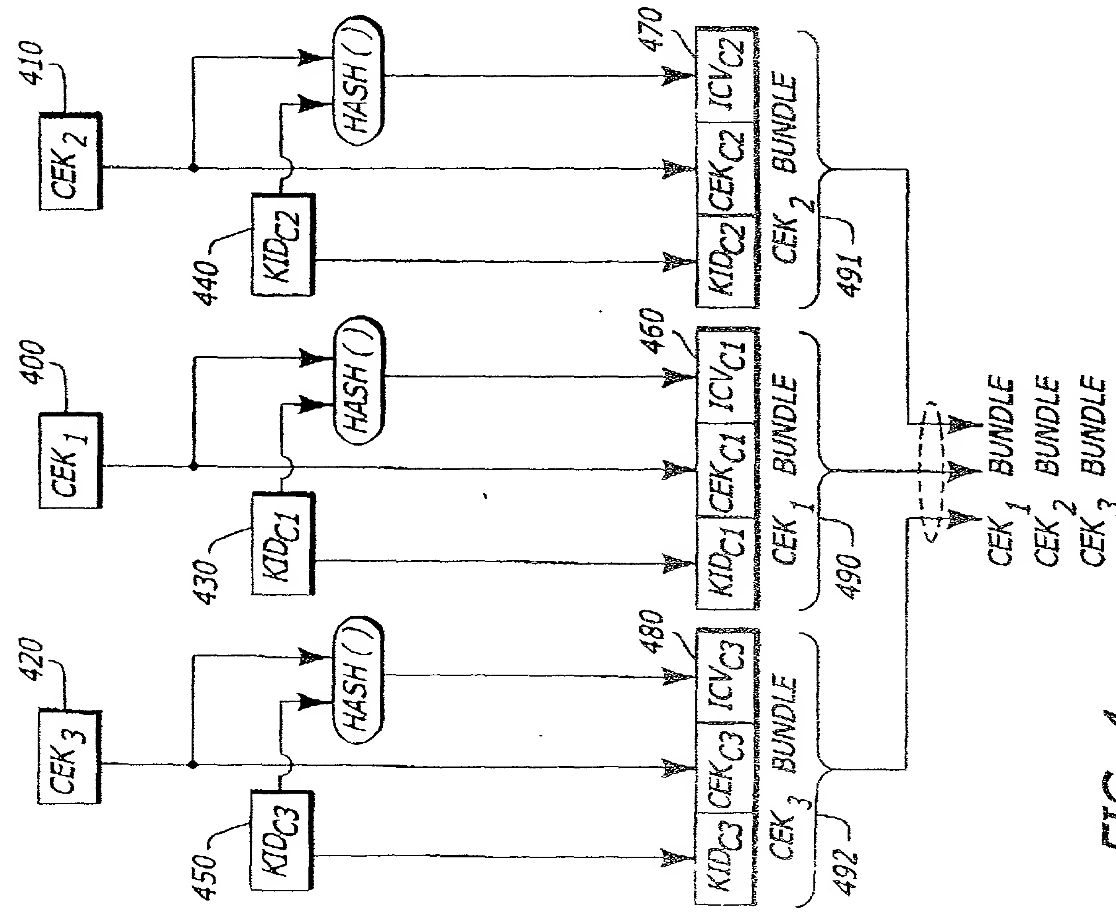

START
PRODUCE BEK_{P1}
PRODUCE BEK_{P2}
PERFORM OPERATION ON BEK_{P1} XOR BEK_{P2} → BEK
END
200
210
220

FIG. 2



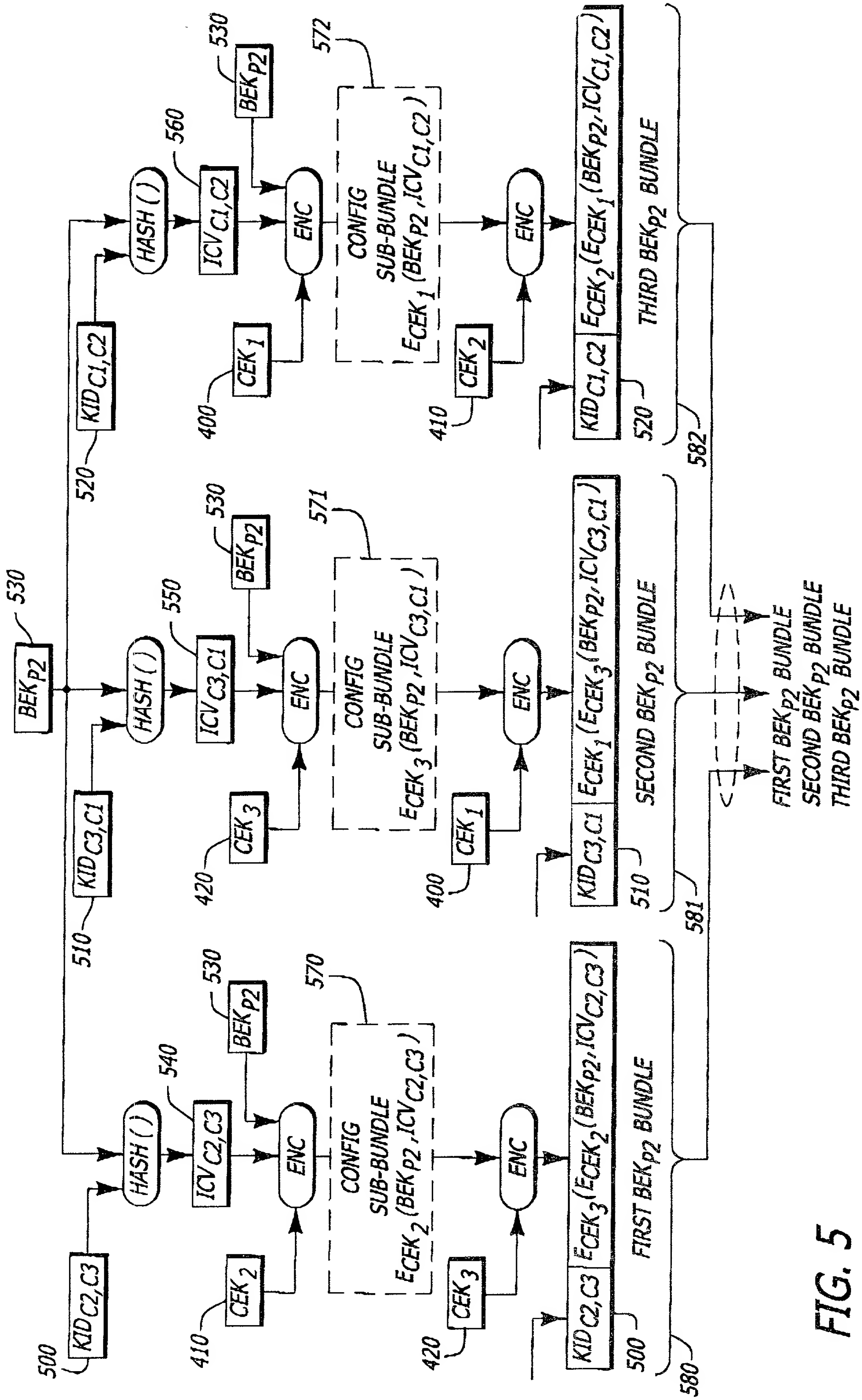
SEK 2
SEK 1
SEK 3
HASH ( )
KID S2
KID S1
KID S3
SEK S2
SEK S1
SEK S3
ICV S2
ICV S1
ICV S3
SEK 2 BUNDLE
SEK 1 BUNDLE
SEK 3 BUNDLE
610
600
620
640
630
650
670
660
680
691
690
692

FIG. 6



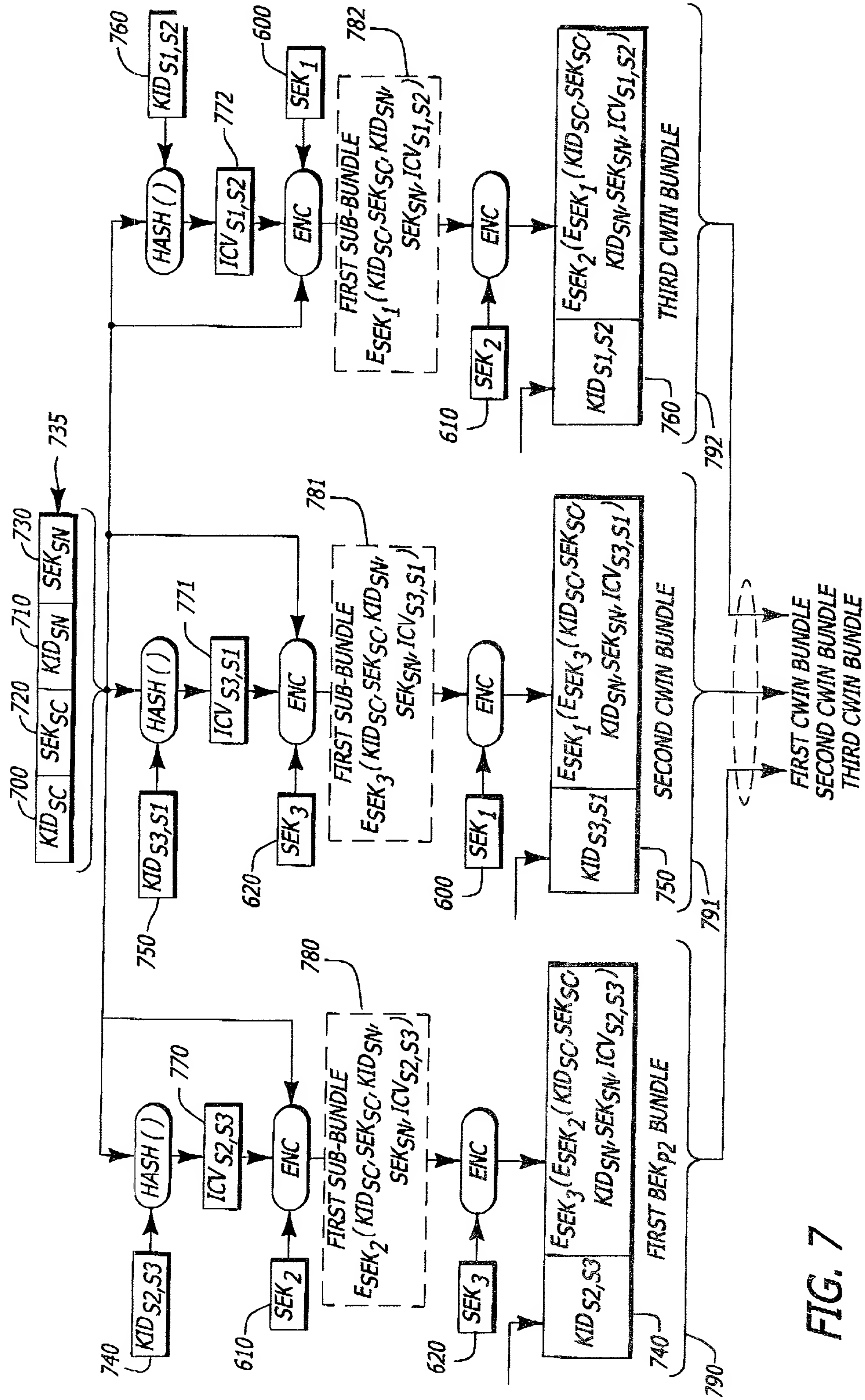
CEK 2
CEK 1
CEK 3
HASH ( )
KID C2
KID C1
KID C3
CEK C2
CEK C1
CEK C3
ICV C2
ICV C1
ICV C3
CEK 2 BUNDLE
CEK 1 BUNDLE
CEK 3 BUNDLE
410
400
420
440
430
450
470
460
480
491
490
492

FIG. 4



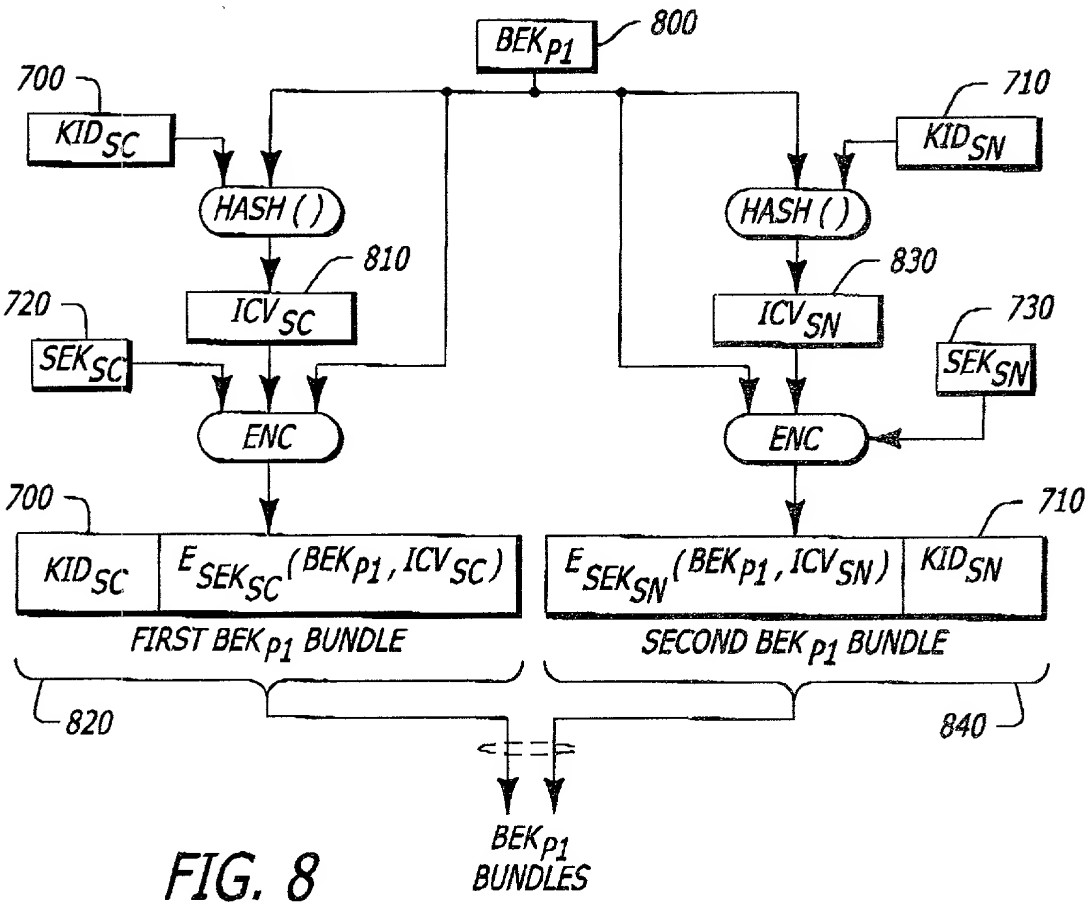
KID C2,C3
HASH ( )
ICV C2,C3
BEK P2
ENC
CEK 2
CONFIG SUB-BUNDLE E CEK 2 (BEK P2 ,ICV C2,C3)
CEK 3
E CEK 3 (E CEK 2 (BEK P2 ,ICV C2,C3)
FIRST BEK P2 BUNDLE
KID C3,C1
ICV C3,C1
CONFIG SUB-BUNDLE E CEK 3 (BEK P2 ,ICV C3,C1)
CEK 1
E CEK 1 (E CEK 3 (BEK P2 ,ICV C3,C1)
SECOND BEK P2 BUNDLE
KID C1,C2
ICV C1,C2
CONFIG SUB-BUNDLE E CEK 1 (BEK P2 ,ICV C1,C2)
E CEK 2 (E CEK 1 (BEK P2 ,ICV C1,C2)
THIRD BEK P2 BUNDLE
FIRST BEK P2 BUNDLE
SECOND BEK P2 BUNDLE
THIRD BEK P2 BUNDLE
500
510
520
530
540
550
560
570
571
572
580
581
582
400
410
420

FIG. 5



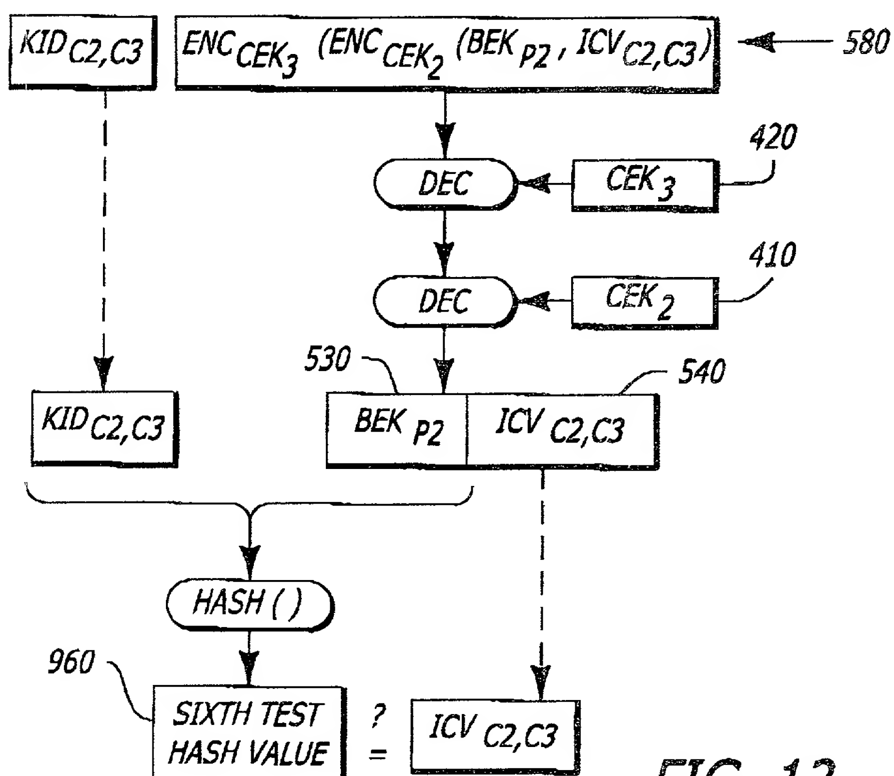
KID SC
SEK SC
KID SN
SEK SN
700
720
710
730
735
KID S2,S3
740
HASH ( )
ICV S2,S3
770
ENC
SEK 2
610
FIRST SUB-BUNDLE
E SEK2 (KID SC, SEK SC, KID SN, SEK SN, ICV S2,S3)
780
SEK 3
620
E SEK3 (E SEK2 (KID SC, SEK SC, KID SN, SEK SN, ICV S2,S3))
FIRST BEK P2 BUNDLE
790
KID S3,S1
750
ICV S3,S1
771
SEK 3
620
E SEK3 (KID SC, SEK SC, KID SN, SEK SN, ICV S3,S1)
781
SEK 1
600
E SEK1 (E SEK3 (KID SC, SEK SC, KID SN, SEK SN, ICV S3,S1))
SECOND CWIN BUNDLE
791
KID S1,S2
760
ICV S1,S2
772
SEK 1
600
E SEK1 (KID SC, SEK SC, KID SN, SEK SN, ICV S1,S2)
782
SEK 2
610
E SEK2 (E SEK1 (KID SC, SEK SC, KID SN, SEK SN, ICV S1,S2))
THIRD CWIN BUNDLE
792
FIRST CWIN BUNDLE
SECOND CWIN BUNDLE
THIRD CWIN BUNDLE

FIG. 7



BEK P1
800
700
KID SC
710
KID SN
HASH ( )
HASH ( )
810
830
720
ICV SC
ICV SN
730
SEK SC
SEK SN
ENC
ENC
700
710
KID SC
E SEK SC (BEK P1 , ICV SC)
E SEK SN (BEK P1 , ICV SN)
KID SN
FIRST BEK P1 BUNDLE
SECOND BEK P1 BUNDLE
820
840
BEK P1
BUNDLES

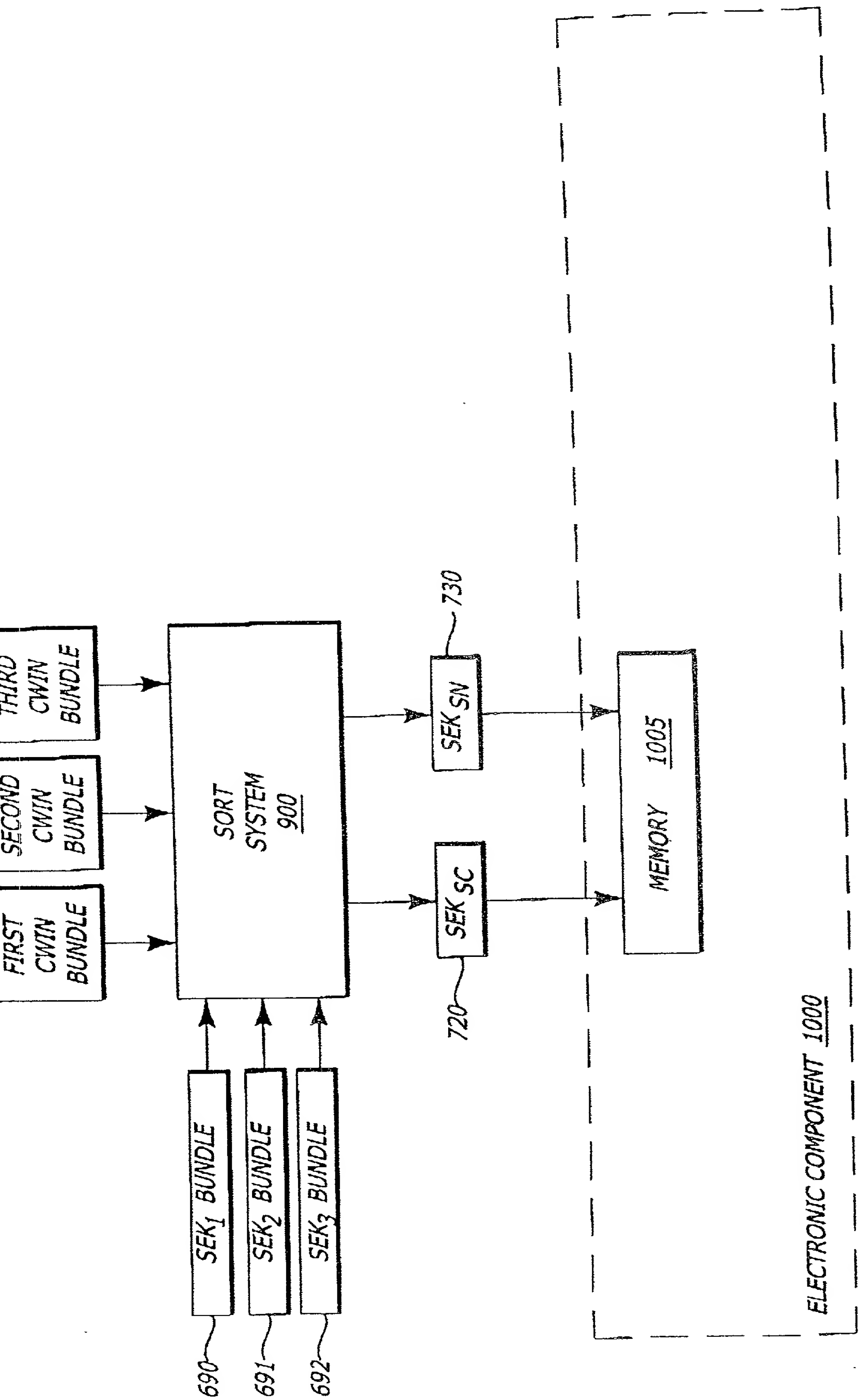
FIG. 8

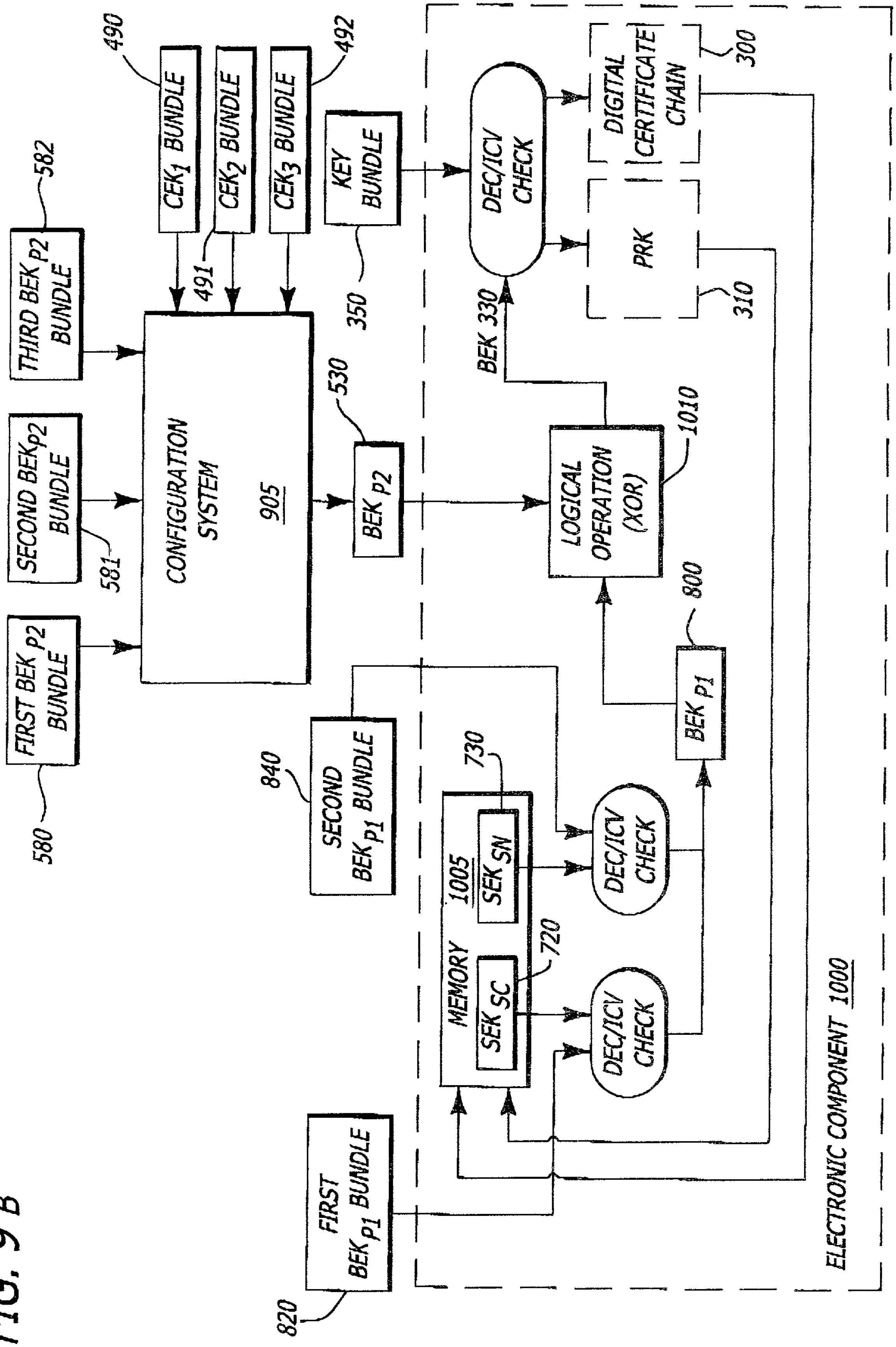


KID C2,C3
ENC CEK3 (ENC CEK2 (BEK P2 , ICV C2,C3)
580
420
DEC
CEK 3
410
DEC
CEK 2
530
540
KID C2,C3
BEK P2
ICV C2,C3
HASH ( )
960
SIXTH TEST
HASH VALUE
?
=
ICV C2,C3

FIG. 13

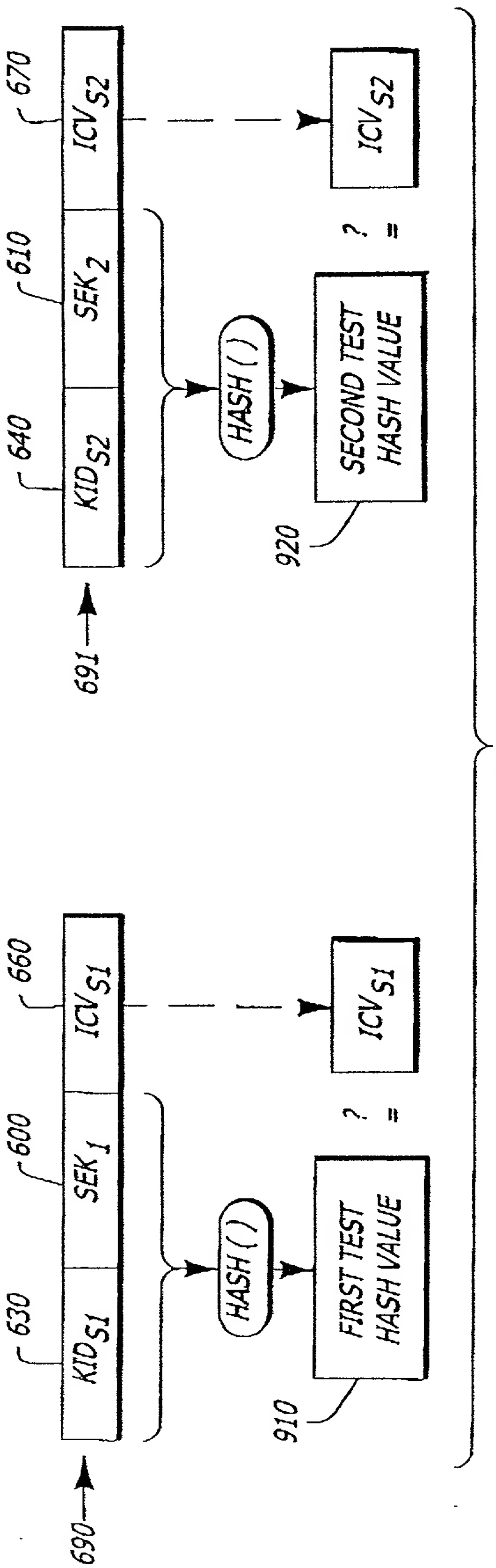
FIG. 9A


FIRST CWIN BUNDLE
790
SECOND CWIN BUNDLE
791
THIRD CWIN BUNDLE
792
SORT SYSTEM 900
SEK SC
720
SEK SN
730
MEMORY 1005
SEK_1 BUNDLE
SEK_2 BUNDLE
SEK_3 BUNDLE
690
691
692
ELECTRONIC COMPONENT 1000



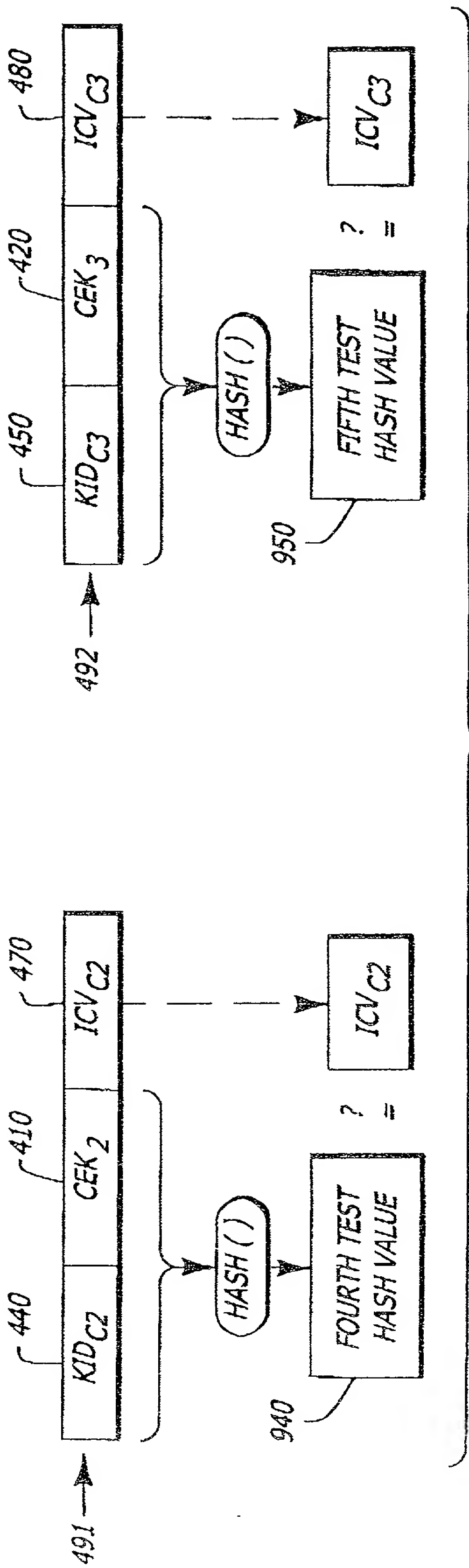
THIRD BEK P2 BUNDLE
582
SECOND BEK P2 BUNDLE
581
FIRST BEK P2 BUNDLE
580
CEK1 BUNDLE
490
CEK2 BUNDLE
491
CEK3 BUNDLE
492
KEY BUNDLE
350
CONFIGURATION SYSTEM
905
BEK P2
530
DEC/ICV CHECK
DIGITAL CERTIFICATE CHAIN
300
PRK
310
BEK 330
LOGICAL OPERATION (XOR)
1010
BEK P1
800
SECOND BEK P1 BUNDLE
840
MEMORY
1005
SEK SN
730
SEK SC
720
DEC/ICV CHECK
DEC/ICV CHECK
FIRST BEK P1 BUNDLE
820
ELECTRONIC COMPONENT 1000

FIG. 9B



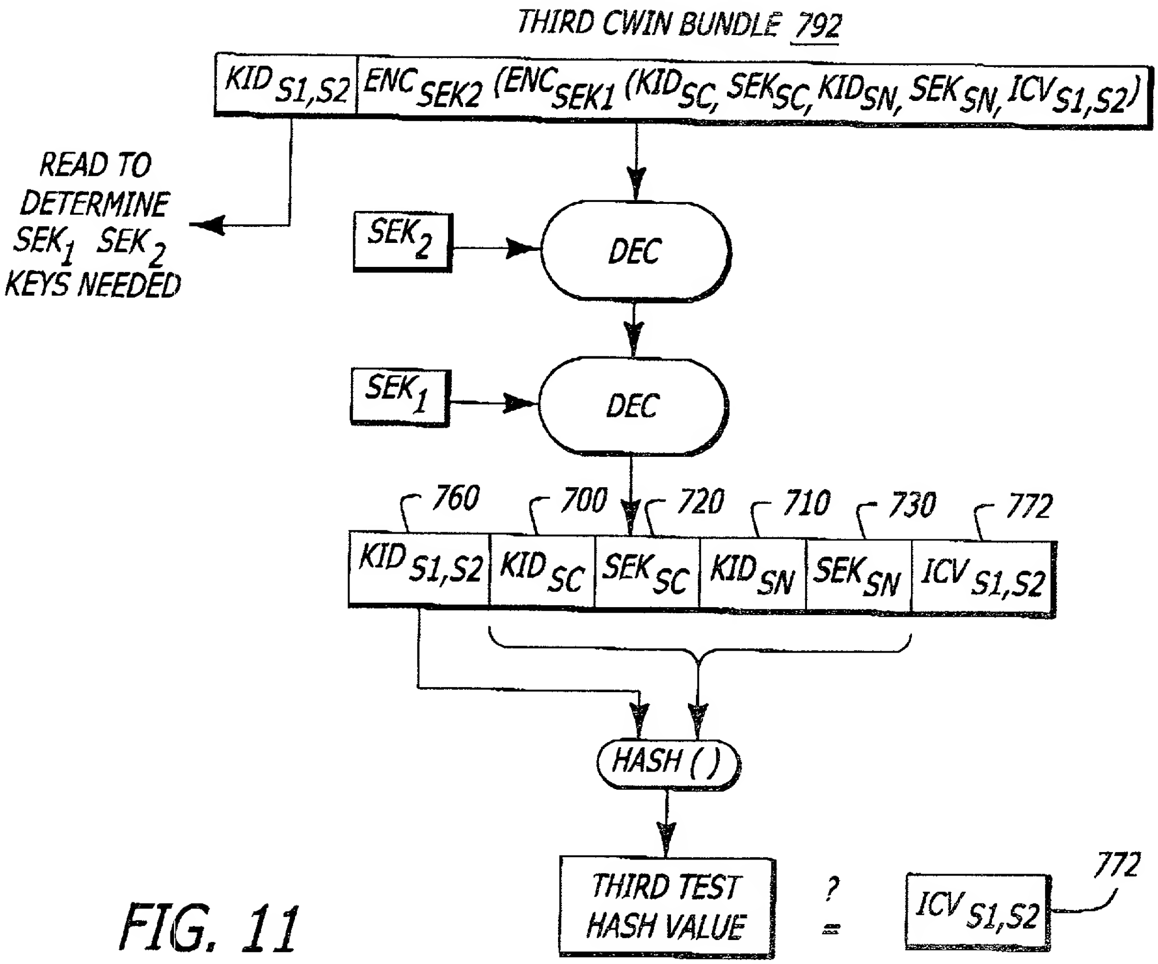
690
630
KIDS1
600
SEK1
660
ICVS1
HASH ( )
FIRST TEST HASH VALUE
910
?
=
ICVS1
691
640
KIDS2
610
SEK2
670
ICVS2
HASH ( )
SECOND TEST HASH VALUE
920
?
=
ICVS2

FIG. 10



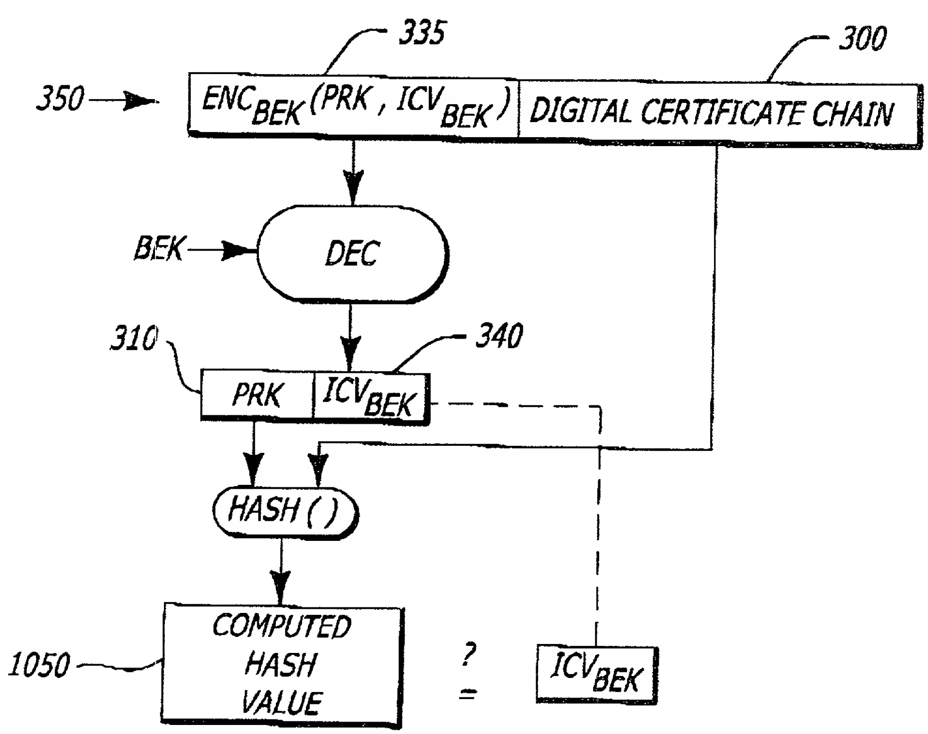
491
440
KIDC2
410
CEK2
470
ICVC2
HASH ( )
FOURTH TEST HASH VALUE
940
?
=
ICVC2
492
450
KIDC3
420
CEK3
480
ICVC3
HASH ( )
FIFTH TEST HASH VALUE
950
?
=
ICVC3

FIG. 12



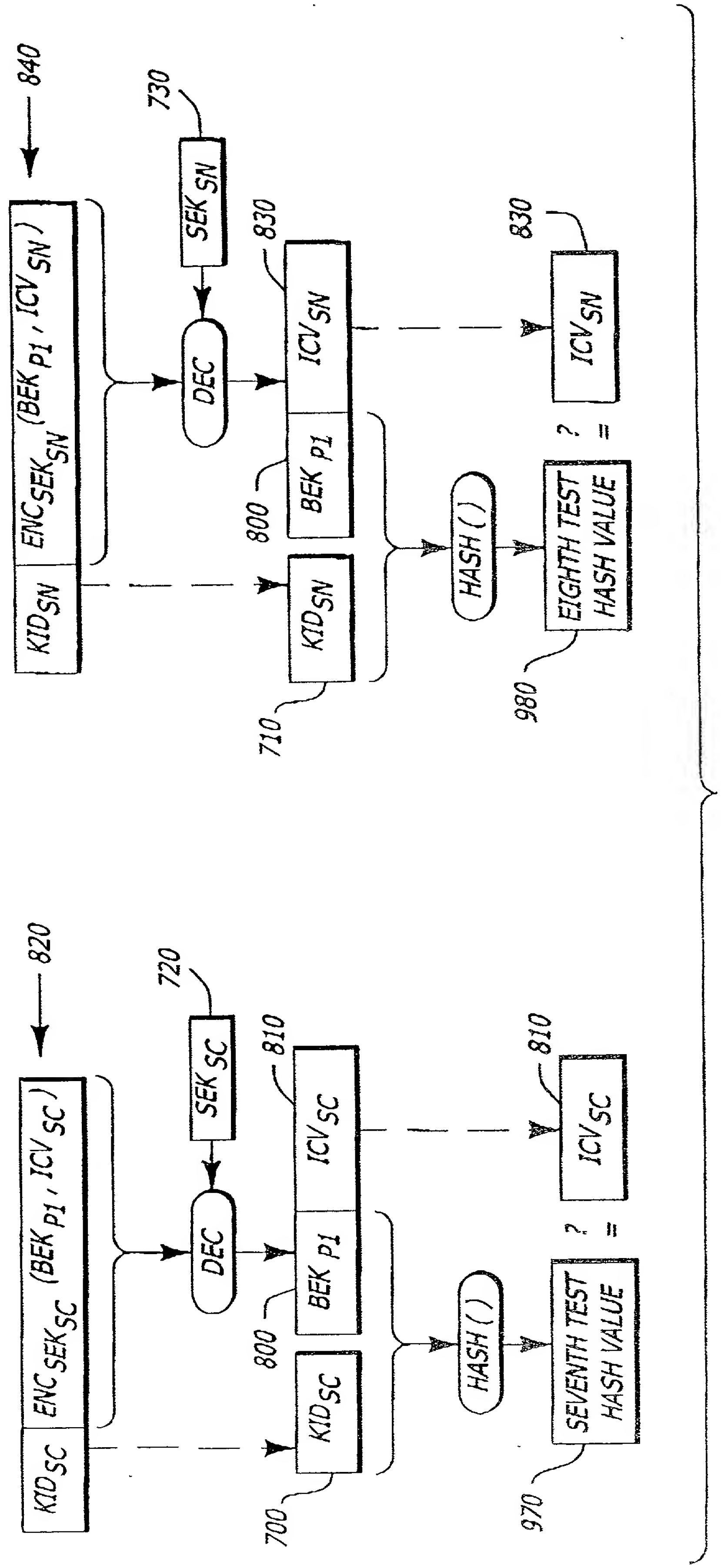
THIRD CWIN BUNDLE 792
KID S1,S2
ENC SEK2 (ENC SEK1 (KID SC, SEK SC, KID SN, SEK SN, ICV S1,S2)
READ TO DETERMINE SEK1 SEK2 KEYS NEEDED
SEK2
DEC
SEK1
DEC
760
700
720
710
730
772
KID S1,S2
KID SC
SEK SC
KID SN
SEK SN
ICV S1,S2
HASH ( )
THIRD TEST HASH VALUE
?
=
ICV S1,S2
772

FIG. 11



335
300
350
ENC BEK (PRK , ICV BEK)
DIGITAL CERTIFICATE CHAIN
BEK
DEC
310
340
PRK
ICV BEK
HASH ( )
1050
COMPUTED HASH VALUE
?
=
ICV BEK

FIG. 15



840
730
SEK_{SN}
KID_{SN}
$ENC_{SEK_{SN}}(BEK_{P1}, ICV_{SN})$
DEC
830
ICV_{SN}
800
BEK_{P1}
KID_{SN}
710
HASH ( )
EIGHTH TEST HASH VALUE
980
?=
830
ICV_{SN}
820
720
SEK_{SC}
KID_{SC}
$ENC_{SEK_{SC}}(BEK_{P1}, ICV_{SC})$
DEC
810
ICV_{SC}
800
BEK_{P1}
KID_{SC}
700
HASH ( )
SEVENTH TEST HASH VALUE
970
?=
810
ICV_{SC}

FIG. 14

DECLARATION AND POWER OF ATTORNEY FOR PATENT APPLICATION
(FOR INTEL CORPORATION PATENT APPLICATIONS)

As a below named inventor, I hereby declare that:

My residence, post office address and citizenship are as stated below, next to my name.

I believe I am the original, first, and sole inventor (if only one name is listed below) or an original, first, and joint inventor (if plural names are listed below) of the subject matter which is claimed and for which a patent is sought on the invention entitled

METHOD FOR SECURE DISTRIBUTION AND CONFIGURATION OF ASYMMETRIC KEYING MATERIAL INTO SEMICONDUCTOR DEVICES

the specification of which

[X] is attached hereto.
[ ] was filed on ______________ as
United States Application Number ______________
or PCT International Application Number ______________
and was amended on ______________.
(if applicable)

I hereby state that I have reviewed and understand the contents of the above-identified specification, including the claim(s), as amended by any amendment referred to above. I do not know and do not believe that the claimed invention was ever known or used in the United States of America before my invention thereof, or patented or described in any printed publication in any country before my invention thereof or more than one year prior to this application, that the same was not in public use or on sale in the United States of America more than one year prior to this application, and that the invention has not been patented or made the subject of an inventor's certificate issued before the date of this application in any country foreign to the United States of America on an application filed by me or my legal representatives or assigns more than twelve months (for a utility patent application) or six months (for a design patent application) prior to this application.

I acknowledge the duty to disclose all information known to me to be material to patentability as defined in Title 37, Code of Federal Regulations, Section 1.56.

I hereby claim foreign priority benefits under Title 35, United States Code, Section 119(a)-(d), of any foreign application(s) for patent or inventor's certificate listed below and have also identified below any foreign application for patent or inventor's certificate having a filing date before that of the application on which priority is claimed:

Prior Foreign Application(s):

APPLICATION NUMBER	COUNTRY (OR INDICATE IF PCT)	DATE OF FILING (day, **month**, year)	PRIORITY CLAIMED UNDER 37 USC 119
			[ ] No [ ] Yes
			[ ] No [ ] Yes
			[ ] No [ ] Yes

I hereby claim the benefit under Title 35, United States Code, Section 119(e) of any United States provisional application(s) listed below:

APPLICATION NUMBER	FILING DATE

I hereby claim the benefit under Title 35, United States Code, Section 120 of any United States application(s) listed below and, insofar as the subject matter of each of the claims of this application is not disclosed in the prior United States application in the manner provided by the first paragraph of Title 35, United States Code, Section 112, I acknowledge the duty to disclose all information known to me to be material to patentability as defined in Title 37, Code of Federal Regulations, Section 1.56 which became available between the filing date of the prior application and the national or PCT international filing date of this application:

APPLICATION NUMBER	FILING DATE	STATUS (ISSUED, PENDING, ABANDONED)

I hereby appoint the persons listed on Appendix A hereto (which is incorporated by reference and a part of this document) as my respective patent attorneys and patent agents, with full power of substitution and revocation, to prosecute this application and to transact all business in the Patent and Trademark Office connected herewith.

Send correspondence to:
William W. Schaal, Reg. No. 39,018, BLAKELY, SOKOLOFF, TAYLOR & ZAFMAN, LLP
(Name of Attorney or Agent)
12400 Wilshire Boulevard, 7th Floor, Los Angeles, California 90025 and direct telephone calls to:
William W. Schaal, (714) 557-3800.
(Name of Attorney or Agent)

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

Full Name of Sole/First Inventor (given name, family name) **Howard C. Herbert**

Inventor's Signature Howard C. Herbert Date 27 June 2000

Residence Phoenix, Arizona USA (City, State) Citizenship USA (Country)

P. O. Address 16817 South 1st Drive

Phoenix, Arizona 85045 USA

Full Name of Second/Joint Inventor (given name, family name) **Derek L. Davis**

Inventor's Signature ________________ Date 27 June 2000

Residence Phoenix, Arizona USA (City, State) Citizenship USA (Country)

P. O. Address 4509 E Desert Trumpet Road

Phoenix, Arizona 85044 USA

Full Name of Third/Joint Inventor (given name, family name) ________________

Inventor's Signature ________________ Date ________________

Residence ________________ (City, State) Citizenship ________________ (Country)

P. O. Address ________________

Full Name of Fourth/Joint Inventor (given name, family name) ________________

Inventor's Signature ________________ Date ________________

Residence ________________ (City, State) Citizenship ________________ (Country)

P. O. Address ________________

Full Name of Fifth/Joint Inventor (given name, family name) ________________

Inventor's Signature ________________ Date ________________

Residence ________________ (City, State) Citizenship ________________ (Country)

P. O. Address ________________

APPENDIX A

I hereby appoint BLAKELY, SOKOLOFF, TAYLOR & ZAFMAN LLP, a firm including: William E. Alford, Reg. No. 37,764; Farzad E. Amini, Reg. No. 42,261; Amy M. Armstrong, Reg. No. 42,265; Aloysius T. C. AuYeung, Reg. No. 35,432; William Thomas Babbitt, Reg. No. 39,591; Carol F. Barry, Reg. No. 41,600; Jordan Michael Becker, Reg. No. 39,602; Bradley J. Bereznak, Reg. No. 33,474; Michael A. Bernadicou, Reg. No. 35,934; Roger W. Blakely, Jr., Reg. No. 25,831; R. Alan Burnett, Reg. No. 46,149; Gregory D. Caldwell, Reg. No. 39,926; Ronald C. Card, Reg. No. 44,587; Thomas M. Coester, Reg. No. 39,637; Donna Jo Coningsby, Reg. No. 41,684; Michael Anthony DeSanctis, Reg. No. 39,957; Daniel M. De Vos, Reg. No. 37,813; Robert Andrew Diehl, Reg. No. 40,992; Matthew C. Fagan, Reg. No. 37,542; Tarek N. Fahmi, Reg. No. 41,402; George L. Fountain, Reg. No. 36,374; Paramita Ghosh, Reg. No. 42,806; James Y. Go, Reg. No. 40,621; James A. Henry, Reg. No. 41,064; Willmore F. Holbrow III, Reg. No. 41,845; Sheryl Sue Holloway, Reg. No. 37,850; George W Hoover II, Reg. No. 32,992; Eric S. Hyman, Reg. No. 30,139; William W. Kidd, Reg. No. 31,772; Sang Hui Kim, Reg. No. 40,450; Walter T. Kim, Reg. No. 42,731; Eric T. King, Reg. No. 44,188; Erica W. Kuo, Reg. No. 42,775; Joseph Lutz, Reg. No. 43,765; Michael J. Mallie, Reg. No. 36,591; Paul A. Mendonsa, Reg. No. 42,879; Clive D. Menezes, Reg. No. 45,493; Darren J. Milliken, Reg. No. 42,004; Chun M. Ng, Reg. No. 36878; Thien T. Nguyen, Reg. No. 43,835; Thinh V. Nguyen, Reg. No. 42,034; Dennis A. Nicholls, Reg. No. 42,036; Lisa A. Norris, Reg. No. 44,976; Daniel E. Ovanezian, Reg. No. 41,236; William F. Ryann, Reg. No. 44,313; James H. Salter, Reg. No. 35,668; William W. Schaal, Reg. No. 39,018; James C. Scheller, Reg. No. 31,195; Jeffrey S. Smith, Reg. No. 39,377; Maria McCormack Sobrino, Reg. No. 31,639; Stanley W. Sokoloff, Reg. No. 25,128; Judith A. Szepesi, Reg. No. 39,393; Vincent P. Tassinari, Reg. No. 42,179; Edwin H. Taylor, Reg. No. 25,129; Joseph A. Twarowski, Reg. No. 42,191; Lester J. Vincent, Reg. No. 31,460; Glenn E. Von Tersch, Reg. No. 41,364; John Patrick Ward, Reg. No. 40,216; Charles T. J. Weigell, Reg. No. 43,398; James M. Wu, Reg. No. 45,241; Steven D. Yates, Reg. No. 42,242; and Norman Zafman, Reg. No. 26,250; my attorneys; and Andrew C. Chen, Reg. No. 43,544; Justin M. Dillon, Reg. No. 42,486; and John F. Travis, Reg. No. 43,203; my patent agents, of BLAKELY, SOKOLOFF, TAYLOR & ZAFMAN LLP, with offices located at 12400 Wilshire Boulevard, 7th Floor, Los Angeles, California 90025, telephone (714) 557-3800, and Alan K. Aldous, Reg. No. 31,905; Robert D. Anderson, Reg. No. 33,826; Joseph R. Bond, Reg. No. 36,458; Richard C. Calderwood, Reg. No. 35,468; Jeffrey S. Draeger, Reg. No. 41,000; Cynthia Thomas Faatz, Reg No. 39,973; Sean Fitzgerald, Reg. No. 32,027; John N. Greaves, Reg. No. 40,362; Seth Z. Kalson, Reg. No. 40,670; David J. Kaplan, Reg. No. 41,105; Charles A. Mirho, Reg. No. 41,199; Leo V. Novakoski, Reg. No. 37,198; Naomi Obinata, Reg. No. 39,320; Thomas C. Reynolds, Reg. No. 32,488; Kenneth M. Seddon, Reg. No. 43,105; Mark Seeley, Reg. No. 32,299; Steven P. Skabrat, Reg. No. 36,279; Howard A. Skaist, Reg. No. 36,008; Steven C. Stewart, Reg. No. 33,555; Raymond J. Werner, Reg. No. 34,752; Robert G. Winkle, Reg. No. 37,474; and Charles K. Young, Reg. No. 39,435; my patent attorneys, and Thomas Raleigh Lane, Reg. No. 42,781; Calvin E. Wells; Reg. No. P43,256, Peter Lam, Reg. No. 44,855; and Gene I. Su, Reg. No. 45,140; my patent agents, of INTEL CORPORATION; and James R. Thein, Reg. No. 31,710, my patent attorney; with full power of substitution and revocation, to prosecute this application and to transact all business in the Patent and Trademark Office connected herewith.